Pedro do Rosário de Brito

Implementação de uma *VLAN*

O caso da Universidade Jean Piaget de Cabo Verde

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

25.5.11

Pedro do Rosário de Brito

Implementação de uma *VLAN*

O Caso da Universidade Jean Piaget de Cabo Verde

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

25.5.11

Pedro do Rosário de Brito, autor da monografia intitulada Implementação de uma *VLAN*, declaro que, salvo fontes devidamente citadas e referidas, o presente documento é fruto do meu trabalho pessoal, individual e original.

Cidade da Praia ao 26 de Maio de 2011
Pedro do Rosário de Brito

Memória Monográfica apresentada à Universidade Jean Piaget de Cabo Verde como parte dos requisitos para a obtenção do grau de Licenciatura em Engenharia de Sistemas e Informática.

Sumário

O trabalho científico de monografia que ora se apresenta, pretende dar a conhecer como as *VLANs* podem ser utilizadas como tecnologia de gestão, monotorização e manutenção da rede. É feito um enquadramento teórico sobre *VLAN*, bem como a sua contextualização num ambiente universitário, mostrando as várias vantagens do uso desta numa rede local, assim como os mecanismos gestão, monotorização e manutenção.

É ainda feito um estudo de caso, sobre uma implementação de uma *VLAN* como mecanismo de gestão, monotorização e manutenção da rede nessa instituição de ensino superior.

Palavras-chave: Redes de computadores, *VLAN*.

Dedicatória

Dedico este trabalho científico aos meus pais, Pedro Alberto de Brito e Maria Jesus do Rosário de Brito por todo investimento, compreensão e confiança que em mim depositaram.

Agradecimentos

Primeiramente agradece a Deus pelo dom da sabedoria e livre atrite, porque sem elas eu não seria o que sou hoje.

Um especial agradecimento a minha orientadora Mestre Fernanda Mascarenhas, pela paciência, pelo incentivo e uma grande virtude e disponibilidade, em me orientar.

Às pessoas da república que para além de amigos, somos uma família. Especialmente minha prima de coração Albertina Duarte, pelo reconhecimento e carinho demostrado.

Um agradecimento a Suzel Andrade pelo empréstimo de uma obra de arte única, o livro de Redes Ciscos. É nesse livro que tive todo o suporte e conhecimento sobre *VLAN*

Um agradecimento de coração a minha namorada Eunice Pereira, pelo apoio incondicional, ternura e amor.

Um agradecimento ao mestre Stefan Monteiro, pelo apoio, pelo tempo e pela amizade.

Como não posso inserir todos aqui, os meus sinceros agradecimentos a todos que directamente ou indirectamente, contribuíram para a realização deste trabalho.

Conteúdo

Tabelas

Figuras

Introdução

1 Contexto

Desde do surgimento das tecnologias, estas vem evoluindo numa escala sem precedentes, tanto que nos últimos séculos viver sem tecnologia é quase impossível. Das tecnologias o que mais destacou foi a rede de computadores, por ter colocado um fim ao isolamento dos computadores. A sua evolução foi tão importante que o seu uso nas organizações é uma necessidade básica mínima. Contudo as redes de computadores também evoluíram, atingindo uma maior capacidade de utilizadores, alargando para grandes áreas geográficas e dividindo em várias redes distintas, destacando as *Local Áreas Network (LAN)* e as *Wide Área Network (WAN)*.

As *LANs* fazem parte das organizações, dando um contribuído muito importante para desenvolvimento das mesmas. As *LANs* transportam grande quantidade de informações, quase de todos os departamentos das organizações, permitindo o acesso a recursos, informações e ainda permitem a partilha dos mesmos de uma forma contínua.

Inicialmente, as *LAN*s das organizações conseguem responder sem problemas aos requisitos das Organizações. Mas com o tempo, e com evolução natural da rede (mais utilizadores, mais dispositivos, etc.), fazer a gestão, manutenção e monotorização, fica um trabalho cada vez mais difícil para o administrador da rede. Para resolver isso foi criada uma nova tecnologia

dentro das redes, designadas *VLAN (Virtual Local área network).* Mas como a tecnologia das *VLAN* pode dar respostas as necessidades actuais exigido pelas evolução das rede?

Para responder a essa questões e outros, foi elaborado esse trabalho científico designado "Implementação de uma *VLAN*, o caso da Universidade Jean Piaget de Cabo verde". A necessidade demonstrada por essa Instituição de Ensino Superior motivou a realização deste trabalho, levando à descoberta de conjuntos de mecanismos para atingir os objectivos pré-estabelecidos durante o estágio na Divisão Tecnológica.

2 Metodologia

Para realização do presente trabalho, foi adaptado as seguintes metodologias:

- Pesquisas Bibliográfica sobre rede de computadores e redes *VLAN*.

- O estudo de caso, na qual se estudou a implementação de uma *VLAN,* de modo a que esta responda aos requisitos da instituição em causa. Para isso foi necessária a utilização de uma ferramenta chamada *Cisco Packet Tracer*. Esta ferramenta permite a simulação da rede, teste e entre outros.

- Construção de um laboratório com ferramentas verdadeiras, como é o caso do *Switch Catalist 2960 séries* da cisco e com alguns PC para testes.

3 Objectivos

3.1 Objectivo geral

- Apresentar uma proposta da criação de uma *VLAN* na rede da Universidade Jean Piaget de Cabo Verde, de modo a que esta seja monitorizada e gerida de uma forma simples e eficaz, de forma a resolver os problemas da Instituição na resolução de falhas na rede actual.

3.2 Objectivos específicos

- Compreender os Mecanismos de funcionamento de uma *VLAN*
- Assimilar as grandes vantagens na implementação de uma *VLAN*
- Identificar os tipos de *VLAN* existentes bem como as metodologias e protocolos que elas usam
- Elaborar um perfil adequado á organização, de modo a que este se encontra organizado funcionalmente
- Compreender os mecanismos de Gestão, monotorização, manutenção das *VLAN* na rede da Intuição

3.3 Estrutura do trabalho

O respectivo trabalho se encontra dividido em 5 partes distintas:

1. **Introdução/Contextualização –** nessa secção faz-se contextualização do tema proposto para investigação, bem como os objectivos do trabalho, e a metodologia usada para a realização do mesmo.

2. **Capitulo 1: Rede de computadores –** nessa secção faz-se um enquadramento geral da rede, desde a sua definição, distribuição geografia, até os tipos de rede que existem. Ainda nessa secção são abordadas um subcapítulo sobre modelo *OSI*.

3. **Capitulo 2: *VLAN* –** nessa parte explica-se o contexto de *VLAN*, dando enfâse as vantagens da sua implementação numa rede local, como também as topologias que ela usa. Descrevesse também dos diferentes tipos de *VLAN* e de como estes se comunicam. Por ultimo, qual mecanismo usado para gestão, configuração e manutenção dos mesmos.

4. **Capitulo 3: O caso da UniPiaget –** nessa secção é apresentado uma proposta de implementação de uma *VLAN*, de modo a que esta se torna segura e estável, de acordo com as necessidades da Universidade. Faz-se um estudo sobre o perfil de cada *VLAN* da instituição. Descreve-se também de mecanismos de monotorização e gestão da *VLAN* no caso da UniPiaget.

5. **Conclusão –** onde é abordada de forma resumida e objectiva, tudo que foi feito nesse trabalho científico, dando enfâse aos objectivos pré-estabelecidos.

Capítulo 1: Redes de computadores

"As redes de comunicação são indispensáveis ao funcionamento de praticamente todas as estruturas da sociedade. No nosso dia-a-dia, é quase certa a utilização de pelo menos um serviço dependente de uma rede de comunicação " (Véstias, 2005).

Dado pela sua importância, ao longo desse capítulo iremos descrever a sua definição, sua estrutura funcional e entre outros. Começando pela sua definição.

De um modo genérico, uma rede não é mais de que um ou mais conjuntos de sistemas ou objectos interligados entre si de modo a poderem partilhar recursos, dados e programas (Gouveia & Magalhães, 2005). Para isso é usado como meio de comunicação os meios como fios de cobre, fibra óptica e actualmente ligação sem fios (*Wireless*), que por sua vez usa ondas de rádio, infravermelhos ou mesmo comunicação via satélite, (Gouveia & Magalhães, 2005).

1 Distribuição Geográfica

Contudo com o tempo, as redes vieram ficar, com diferentes tamanhos, originando assim a necessidade de os organizar pelo espaço ocupado geograficamente (Tanenbaum, 1996).

Inicialmente existiam três nomenclaturas na destruição geográfica, sendo elas as *LAN (Local Area Network),* as *MAN (Metropolitan Area Network)* e as *WAN (Wide Area Network)* (Tanenbaum, 1996).

Mas com o passar do tempo e a evolução das tecnologias de comunicação, a nomenclatura *MAN* foi eliminado, ficando assim só as *LAN* e *WAN* (Gouveia & Magalhães, 2005).

Contudo será feito a descrição de todas nomenclaturas começando pelas *LAN* até *WAN*

1.1 *LAN – Local Area Network*

As *LAN* surgiram no ano 1970 para terminar o isolamento de comutadores. Contudo nessa altura, a interligação era possível somente nas máquinas dos mesmos fabricantes, mas com o aparecimento da *ETHERNET* esse problema foi ultrapassado (Sá, 2007).

Uma *LAN* serve para ligação de vários dispositivos numa curta área. Estas áreas podem ocupar um escritório, um edifício, ou até um campus universitário, (Gouveia, et al., 2005). Mas e bom salientar que isto não implica que a rede seja pequena. Ela pode conter vários dispositivos ligados, só que este se encontra próximo um dos outros (Lowe, 2008).

1.2 *MAN – Metropolitan Area Network*

A *MAN* é uma versão ampliada de uma *LAN*, só que este consegue abranger um conjunto de escritórios vizinhos ou uma cidade inteira, ou seja uma *MAN* é a ligação de dois ou mais *LAN*, através de um dispositivo de comunicação (*router* e *modems*), (Tanenbaum, 1996).

Mas como foi referido no subcapítulo da “Distribuição Geográfica” as *MAN* foram eliminados com a evolução e inserção de novas tecnologias.

1.3 *WAN - Wide Area Network*

Com o crescimento de várias organizações, houve a necessidade de dispersão das suas instalações por locais geográficos distantes, por vezes para outros continentes. Contudo por motivos técnicas e económicas, as *LAN* não eram adequados para comunicações de longo alcanço, por isso nasceram as *WAN* (Gouveia & Magalhães, 2005).

De uma forma resumida, as *WAN* são nada mais, nada menos de que uma infra-estrutura que consegue suporte um conjunto de *LANs* e tendo de cobertura bastante grande geograficamente, cobrindo um país, um continente, ou até mesmo vários continentes. Um exemplo bastante claro de uma *WAN* é a *Internet* (Barros, 2007).

2 Topologias de rede

Depois de ser descrito a distribuição geográfica de uma rede, será feito a descrição da sua topologia.

De uma forma genérica, uma topologia refere à forma de como os dispositivos de rede se encontra conectados uns aos outros e de que modo os mesmos se comunicam entre si (Lowe, 2008).

Contudo a escolha de uma boa topologia vária na relação entre dois elementos chaves, a eficiência e velocidade, ou seja a escolha de uma topologia para uma rede vai depender da sua eficiência na transmissão/recepção dos dados e da sua velocidade para o mesmo (Soares, Lemos, & Colcher, 1995).

A escolha errada de uma topologia pode originar mais tarde a custos desnecessários assim como um mau aproveitamento dos recursos da rede. Para tal existem vários tipos de topologia sendo estes três os mais comuns (Gouveia & Magalhães, 2005):

- Topologia em Barreamento
- Topologia em Estrela
- Topologia em Anel

Será feito uma breve descrição dessas topologias e depois o levantado alguns pontos fortes e fracos dessas topologias de acordo com os seus componentes fisicos.

2.1 Topologia em Barramento – *Bus Topology*

A topologia em barramento tem como base que todos os dispositivos de rede se encontram ligados através de um único cabo (Lowe, 2008), ou seja nessa topologia todos os dispositivos estão conectados a um cabo continua que é terminado em ambos as extremidades por uma pequena

ficha de resistência, ligada entre a malha e o fio central do cabo, (Gouveia & Magalhães, 2005). A comunicação é feita por *broadcast*, ou seja os dados é visto por todos os computadores, mas só serão recebidos pelo destinatário.

Contudo este tipo de topologia caiu em desuso devido a evolução tecnológica (Loureiro, 2003).

- **Pontos Fortes** (Gouveia & Magalhães, 2005)
  - ✓ A facilitação de instalação
  - ✓ É relativamente económico
  - ✓ Usa menos cabos do que outras topologias
- **Pontos Fracos** (Gouveia & Magalhães, 2005)
  - ✓ A dificuldade de mudar ou mover nós
  - ✓ Praticamente não tem tolerância a falhas, caso de falha um dos nós toda a rede a rede vai abaixo
  - ✓ Dificuldade de diagnosticar falhas ou erros

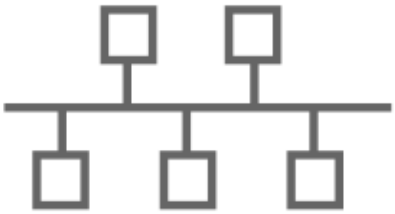


Figura 1 – Topologia em Barramento
Fonte: adaptado de (Barros, 2007)

2.2 Topologia em Estrela – *Star topology*

Relativamente a topologia *Bus* a topologia *Star* apresenta uma maior flexibilidade na alteração da estrutura da rede, e consequentemente é aquele que é usado em quase em todas as redes *Ethernet* (Loureiro, 2003). Ela une os dispositivos de rede através de um dispositivo de comunicação (*switch* ou *hub*) central (ou simplesmente nó central), na qual sai um cabo para cada dispositivo de rede, formando assim uma estrela, nome pela qual é designado (Loureiro, 2003). Com a evolução da rede, a administrador da rede tem a necessidade de expandir a sua

rede, ficando assim em vez de um no central, dois nós central, a qual designamos “topologia de estrela estendida” ou *Expending Star topology* (Lowe, 2008).

- **Pontos Fortes** (Gouveia & Magalhães, 2005)

  - ✓ Facilidade de modificação de sistema, já que todos os cabos convergem para um só ponto
  - ✓ Um dispositivo por derivação, se esta falhar só esse dispositivo é afectado
  - ✓ Fácil detecção e isolamento de falhas, dado que o nó central está directamente ligado a todos os outros
  - ✓ Simplicidade do protocolo de comunicações resume-se a seleccionar qual o nó periférico que em cada momento está ligado ao nó central

- **Pontos Fracos** (Gouveia & Magalhães, 2005)

  - ✓ Maior comprimento de cabo para efectuar as ligações
  - ✓ Dependência do nó central, se este falha, a rede fica inoperacional

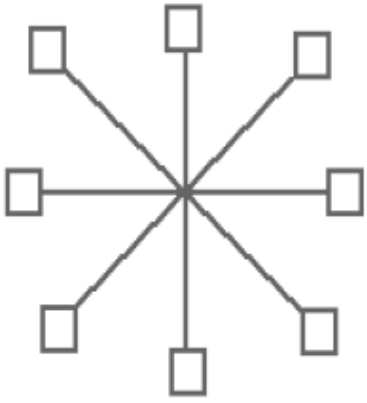


Figura 2 – Topologia em Estrela
Fonte adaptado de (Barros, 2007)

2.3 Topologia em Anel – *Ring Topology*

A topologia em anel consiste em um caminho fechado, por onde os dispositivos se conectam, assim podem receber/transmitir dados em ambos direcções (Soares, Lemos, & Colcher, 1995). Os dados circulam de um posto para outro, e cada posto inclui um dispositivo de recepção e transmissão, o que lhe permite receber a informação e passá-lo ao posto seguinte, no caso de a informação não lhe ser destinada (Gouveia & Magalhães, 2005).

- **Pontos Fortes** (Gouveia & Magalhães, 2005)
  - ✓ Pequeno comprimento de cabo
  - ✓ Não são necessários armários de distribuição de cabos, dado que as ligações são efectuadas em cada um dos nós.
  - ✓ O desenho da cablagem é bastante simples
- **Pontos Fracos** (Gouveia & Magalhães, 2005)
  - ✓ A falha de um nó provoca a falha da rede
  - ✓ Dificuldade de localização de falhas (a falha de nó provoca a falha de todos os outros)
  - ✓ Dificuldade em reconfiguração a rede (instalação de vários nós em locais diferentes)

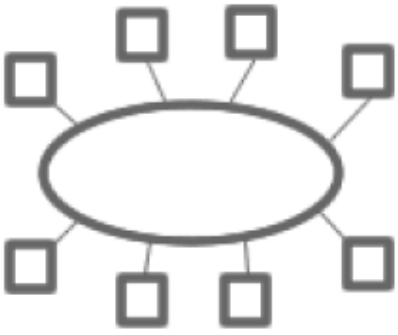


Figura 3 – Topologia em Anel
Fonte: adaptado de (Barros, 2007)

3 O Modelo *OSI - Open Systems Interconnection Model*

Antes de descrever o modelo *OSI*, será descrito um pouco o que são protocolos.

Nos subcapítulos acima, foi ilustrado como os dispositivos se encontram situados geograficamente e topologicamente, mas ainda não foi referido como os mesmos se conseguem comunicar, transmitir dados, sabendo que podem ser feitos de fabricantes diferentes. Para isso é que existem protocolos e normas.

De um modo geral protocolos e normas é que fazem as redes trabalharem como um único conjunto. Os protocolos são um conjunto de regras que permitem a comunicação eficaz entre vários dispositivos de uma rede. As normas fazem também que os dispositivos de rede se comunicam, mas dando enfâse a dispositivos com fabricantes diferentes (Lowe, 2008).

No início, cada organização fabricava os seus protocolos, ficando assim difícil a comunicação de vários tipos de componentes de rede. Foi nessa necessidade que foram criados protocolos padrão (*standard*), que são protocolos a nível mundial que permitem que diferentes tipos de componentes de rede, mesmo que sejam de fabricantes diferentes. Um claro exemplo desse tipo de protocolo padrão é o modelo *OSI* (Lowe, 2008).

O modelo *OSI* foi criado pela *ISO* (*Internacioanal Standards Organization*) com finalidade de normalizar a corrente de informação em diferentes máquinas numa rede (Gouveia & Magalhães, 2005). O modelo foi desenvolvido nos finais dos anos setenta, e ela quebra vários aspectos da rede em sete camadas distintas, como é ilustrada na Figura 4 (Loureiro, 2003).

Figura 4 – Modelo *OSI*

Fonte: adaptado de (Pinto, 2010)

A descrição de cada uma dessas camadas serão pronunciados no supcapitulo seguinte, intitulado Camadas do modelo *OSI*.

3.1 Camadas do modelo *OSI*

Como foi ilustrado na Figura 4 o modelo *OSI* se encontra subdivido em sete camadas distintas. Durante este subcapítulo será descrevido essas camadas uma por uma e dando uma pequena descrição, o que cada uma representa.

Será feito uma descrição das camadas mais acima (aplicação) e de uma forma contínua até descer-nos de níveis até atingirmos a ultima camada (física).

- **Camada da Aplicação – *The Application layer***

A camada da aplicação é a camada supeiror do modelo *OSI*. É nela que se define quais os protocolos a utilizar para determinadas tarefas, e tem a resposanbilidade de definir como a acções se interagem na rede (Gouveia & Magalhães, 2005).

Ou seja, esta camada apresenta o *software* a qual as aplicações recorem para aceder a recursos da rede (Loureiro, 2003), e para isso é ussada um conjunto de serviços de comunicação (Véstias, 2005).

Aqui vai uma pequena lista dos protocolos mais ussados pela camada da aplicação (Lowe, 2008):

  - ***DNS (Domain Name System)*** para resolução de nomes do dominio da rede e da internet
  - ***FTP (File Transfer Protocol)*** para transferencia de ficheiros
  - ***SMTP (Simple Mail Transfer Protocol)*** para email
  - ***Telnet*** para emulação de terminal

- **Camada de Aplicação – *The Presentation layer***

A camada de aplicacação é responsavel pela converção de dados, pela encripitação, compreenção de informações, de modo a que estes sejam transferidos de forma mais rapido (Gouveia & Magalhães, 2005).

Uma sua caracteristica dessa camada é possibilidade de efectuar a transação de carctéres, por exemplo, do código *ASCII (American Standard Code for Information Interchange),* para *EBCDIC (Estended Binary Coded Decimal Interchange Code)* e vice-versa (Lowe, 2008). Esta converção é necessario devido a incompatibilidade de diferentes sistemas.

- **Camada de Sessão – *The Session Layer***

A camada de sessão é reponsavel por inciar, controlar e terminir trocas de dados. Tendo como objectivo principal a troca a conversão de dados das aplicações, num formado reconhecido pelas ambos entidades (Véstias, 2005). Ou seja, a camada de sessção define como dois dispositivos estabelecem uma ligação, com segurança, transferencia, coneção de dados, e por ultimo verificar se os mesmos não contém erros (Gouveia & Magalhães, 2005).

Aqui vai uma pequena lista dos protocolos mais ussados pela camada da secção (Gouveia & Magalhães, 2005):

  - ***HTPP (Hyper Test Transfer Protocol***)
  - ***TFTP (Trivial File Transfer Protocol)***
  - ***MIME (Multipurpose Internet Mail Extension)***
  - ***NFS (Network File System)***

- **Camada de Transporte - *The Transpot Layer***

A camada de Transporte junta dados recebidos pela camada de sessão numa única fila de dados. Este dados são segnemtados pelo emissor antes de serem enviados pela camada inferior (camada de rede) e reagrupados pelo receptor antes de serem encaminhados pela camada superior (camada de sessão) (Véstias, 2005).

Por outras palavras a camada de transporte é responsável para verificar se a informação foi entregue sem erro para o destinario. Para isso ela segmenta a informação em pequenos segmentos que serão agrupados novamente no destinatario (Gouveia & Magalhães, 2005).

E nessa camda são mais usado este dois tipo de protocolos (Véstias, 2005):

  - ***TCP(Tranfer Control Protocol)*** com confirmação da recepção
  - ***UDP(User Datagram Protocol)*** sem confirmação da recepção

- **Camada de Rede – *The Network Layer***

"A camada de rede é responsavel pelo endereçamento lógico e efectuar a transição de nome lógicos para endereços fisicos." (Gouveia & Magalhães, 2005), ou seja a camada de rede tem a responsabilidade de identificar todas as entidades da comunicação, verificando o endereço logico, e a partir desse endereço determinar o melhor caminho entre as entidades envolventes na comunicação (Véstias, 2005).

Ela também define o modo de fragmentação de dados em pacotos de dados, de modo a este seja a unidade maxima transmitida suportada pelos dispositivos da rede (Véstias, 2005).

Normalmente os dispositvos que se comunicam entre si, enviam sempre o seu *MAC address* para a rede e só depois o numero de *IP*, mais conhecido pelo indereço logico. Apesar que os *MAC address* sejam unicos a cada placa de rede, podem vir existir conflitos de endereçamento logico se estes foram os mesmo dentro de uma rede (Gouveia & Magalhães, 2005). Por trabalhar com endereço lógico ela usa o protocolo *TCP/IP* para fazer a comunicação entre os diferentes dispositivos (Loureiro, 2003).

- **Camada de Ligação de Dados – *The Data Link Layer***

A camada de ligação de Dados, recebe os dados da camada da rede e transforma-las em unidades designadas *tramas/frames e* vice-*versa*. Na *trama* contem indentificadores que identifica o início o fim do mesmo, bem como outros campos, como o campo de endereçamento físico de origem e destino dos dispositivos em comunicação (Véstias, 2005).

Eis exemplo de alguns protocolos que ela usa (Véstias, 2005):

  - ***HDLC (High-level Data Link Control)***

  - ***PPP (Point-to-Point Protocol)***

- **Camada Física – *The Physical Layer***

A camada Física é a camada mais baixo do modelo *OSI* e não obedece a nenhum protocolo específico e ela funciona de acordo a comunicação física estabelecida com os dispositivos

intermediários (Gouveia & Magalhães, 2005). Ou seja responde ao adaptador da rede, ela manipula sinais eléctricos que passam na rede, lendo e escrevendo conjuntos de uns e zeros (linguagem maquina) (Loureiro, 2003).

4 Considerações finais

No capítulo da rede foi elaborado vários assuntos sobre a rede de computadores, desde da definição, topologias, distribuição geografia, etc., entre outros. Também foi referenciado o modelo *OSI* e as suas camadas e descrição.

Contudo e bom salientar que apesar desses atributos, a arquitectura da rede esta sempre a sofrer alterações, mudando de topologia, de termologia devido a aparecimento de novos atributos. Mas o uso de rede é ainda extramente essencial, e a sua implementação deve ser analisada antes da sua implementação, evitando assim alguns contornos mais logos, e de ter em sempre em conta a evolução da rede (mais utilizador, mais dispositivos). A evolução é necessária, e precisamos estar prontas quando elas vêm. A rede deve estar preparada para futuras alterações, e dar respostas a todas as necessidades da organização.

Em relação ao modelo *OSI*, a sua compreensão é extramente importante para um bom conhecimento e funcionamento da rede, e como os dispositivos se comunicam. Qualquer que seja o administrador da rede deve conhecer todas as camadas do modelo *OSI* e função de cada uma delas, e como e estabelecido a comunicação entre cada camada do modelo *OSI*.

Capítulo 2: *VLAN*

Antes de se abordar as *VLAN*, será feito uma descrição geral do *Switch*, bem como do seu funcionamento na utilização da sua tabela.

O *Switch* serve para ligar vários segmentos da rede, estabelecendo uma ligação directa entre o dispositivo transmissor e o dispositivo receptor (Gouveia & Magalhães, 2005). Ou seja o *Switch*, é o dispositivo (comutador) intermidiário que liga um dispositivo final ou um conjunto de dispositivos finais a outro dispositivo finais ou conjuntos de dispositivos finais de modo a estes permanecer numa ligação de diálogo directo.

Para entender melhor o funcionamento do *Switch*, temos de compreender o processo de tabela de encaminhamento. É nesse processo que o Switch aprende a econtrar a porta correcta para fazer a ligação directa entre o emissor e o receptor (Farias, 2006). Para compreender isso melhor vamos seguir este exemplo ilustrado na Tabela 1.

Dispositivo	**Endereço MAC**	**Porta**
PC-João	0001	1
PC-Ana	0002	2
PC-Maria	0003	3

Tabela 1 – Tabela de *Switch*

Na Tabela 1 temos três dispositivos, PC-João, PC-Ana e PC-Maria. O PC-João tem uma placa de rede com um endereço MAC 0001 ligada na porta 1 do *Switch*, enquanto o PC-Ana tem

uma placa de rede como endereço MAC 0002 e se encontra ligada na porta 2, e por fim o PC-Maria tem como endereço MAC0003 e se encontra ligado na porta 3 do mesmo *Switch*. Contudo a tabela do Switch se encontra vazia, quando este é reiniciado pela primeira vez.

O PC-João pretende comunicar com o PC-Maria, para isso ele cria um *frame* com as informações necessárias para houver comunicação, como e ilustrado na Tabela 2, e envia o *frame* em *broadcast* para todas as portas do Switch.

Endereço MAC Origem	Endereço MAC Destino
0001	0003

Tabela 2 – *Frame* do PC-João

Este *frame* inicializa a tabela do *Switch* com os dados do seu endereço MAC e porta do dispositivo como é ilustrado na Tabela 3.

Dispositivo	Endereço MAC	Porta
PC-João	0001	1

Tabela 3 – Tabela do *Switch* actualizado com PC-João

Como o *frame* é descartado pelos outros dispositivos (PC-Ana neste expecifico caso), o dispositivo PC-Maria responde ao pedido do *frame*, actualizando assim a tabela do Switch, liberando dados como endereço MAC e a porta para a tabela do *Switch*, como é ilustrado na tabela 4.

Dispositivo	Endereço MAC	Porta
PC-João	0001	1
PC-Maria	0003	3

Tabela 4 – Tabela do *Switch* actualizado com PC-João e PC-Maria

Quando o dispositivo PC-João e PC-Maria precisarem se comunicar novamente, o *Switch* não mais enviará o *frame* para todas as portas, e sim e tão somente entre as portas de que PC-João e PC-Maria fazem parte. Em suma, o *Switch* utiliza o Endereço MAC de origem para aprender os endereços e o Endereço MAC de destino para comutação dos *frames*.

1 Fundamentos e conceitos

Depois de ter descrito o funcionamento do *Switch* e ter descrito as redes de computadores, da sua topologia e dos seus protocolos, será descrito nesse capítulo 2, uma das particularidades da *LAN*, que é as *VLAN*.

" (…) por defeito, todos os *Switch* de uma rede pertencem ao mesmo domínio de *broadcast*." (Véstias, 2005), ou seja que todo ou qualquer pacote enviado para o domínio de *broadcast,* é enviado para toda a rede através dos *Switches,* originando assim paralisação da rede.

Contudo o mesmo não é grave numa rede de poucas dimensões ou *broadcast* reduzido. Mas no mundo de hoje, existem um grande número de aplicações, mais especificamente as aplicações multimédias que usam *broadcast* e *multicast* intensivamente (Véstias, 2005).

E para resolução desse tipo de problemas, surgiram as *VLAN – Virtual Local Area Network* ou *Virtual LAN* como tecnologia para resolução deste tipo de problemas, entre outros. Contudo e bom salientar que a tecnologia da *VLAN* não serve só para resolver conflitos de domínios de *broadcast.* Pode ainda ser usado como um mecanismo de controlo e gestão da rede de uma organização como podemos demonstrar durante o capítulo 2. Mas contudo, o que são as *VLAN?*

VLAN "é uma rede local que agrupa um conjunto de máquinas de maneira lógica e não física". Por conseguinte, ela tornasse mais flexível quando se trata na gestão da rede, utilizando como base um conjunto de normas (PILLOU, 2009).

O mesmo é definido por (Zacaron, 2007), definindo que uma *VLAN* é um agrupamento lógico de postos ou dispositivos de rede. Estes podem ser agrupados por funções operacionais ou por departamentos de uma forma lógica e não fisicamente.

O mesmo opina que é proibida a comunicação entre *VLAN* diferentes, contudo isso pode ser feito através de um *router*, e somente em casos autorizados.

Com base nas definições dos autores acima, podemos afirmar que uma *VLAN* é uma segmentação de uma única *LAN* física em diversas *LAN* lógicas, sendo que estes últimos comportam como *LAN* física diferentes. Desta forma cada *LAN* lógica não pode comunicar com as outras *LAN,* a não ser que usam um dispositivo de camada três do modelo *OSI* (*Switch* ou *router*) e com permissão para a conexão.

2 Topologias de *VLAN*

Depois de ver a definição de *VLAN*, será descrevido a sua topologia.

Até hoje em dia existem três tipos de topologia de *VLAN* sendo elas as seguintes (Zacaron, 2007):

- *VLAN* baseado em Porta
- *VLAN* baseado em Endereços MAC
- *VLAN* baseado em Protocolos

Nas secções seguintes, cada uma das *VLANs* serão analisados com maior detalhe.

2.1 *VLAN* baseado em Porta – *Port-Based* ou *Port-Centric VLAN*

VLAN baseado em porta é quando um dispositivo se conecta a uma infra-estrutura de rede, ela é associado automaticamente a *VLAN* da qual a porta que se encontra configurada (Zacaron, 2007). Por outras palavras, se o dispositivo se encontra ligado a uma porta do *Switch* e esta porta encontra-se configurada para *VLAN2*, então este dispositivo pertence a um segmento da rede onde se encontram um grupo de dispositivos que se encontram associados a *VLAN*2.

A topologia baseada por porta é tão utilizada, que a maioria dos fabricantes de segmentação da rede padronizou-a por defeito nos equipamentos que suportam *VLAN* (Cisco Systems Inc, 2003). Ou seja, por defeito a maioria dos *switches* vem com configuração por porta (normalmente *VLAN1*), á qual todas as portas se associam automaticamente.

Contudo um dos pontos fortes no uso dessa topologia é que quando uma porta é associada a uma *VLAN* específica, o mesmo é independente de utilizador que não reconhece a existem do *VLAN*, consequentemente isto mantém as tabelas de consulta menos complexas (Zacaron, 2007).

Por outro lado, o mesmo constata que o uso dessa topologia requer que os dispositivos estejam ligados sempre no mesmo lugar e qualquer mudança de lugar, poderá originar uma nova configuração das tabelas de consulta do *Switche* (Zacaron, 2007).

A Tabela 5 demonstra um exemplo de uma *VLAN* de topologia por Porta num *switch* de 16 portas.

Portas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
VLAN	3	2	1	1	3	1	2	2	2	1	3	3	3	1	2	2

Tabela 5 – Associação de portas para cada *VLAN*

Para melhor entender a Tabela 5, será feito uma descrição melhor dessa tabela, começando pela porta 1 do *Switch,* que se encontra configurado para o segmento da rede pertencendo a *VLAN3,* a porta 2 do *Stwich* se encontra configurada para o segmento da rede pertencendo *VLAN2,* enquanto a porta 3 do *Switch* se encontra configurada para o segmento da rede pertencendo a *VLAN1,* e assim por adiantes durante toda as portas do *Switch.* Assim o dispositivo que conectar a porta 3 e porta 4 do *Switch* encontrasse no mesmo segmento da rede *VLAN*1, o mesmo não aplica ao dispositivo que se encontra conectado porta 1 do *Switch.*

2.2 *VLAN* baseado em Endereços *MAC – MAC Address-Based VLAN*

Um dispositivo ao se conectar a uma porta de *Switch,* envia o seu endereço *MAC* (*Media Access Control*) para a tabela do *Switch*. O *MAC* do dispositivo é verificado numa base de dados de um servidor, de forma a associar-se ao segmento de rede configurado no servidor(Zacaron, 2007). Ou seja, quando um dispositivo se conecta a um *Switch,* configurado por *VLAN* baseado em endereço *MAC,* esta inicializa um processo de consulta à base de dados do servidor, comparando o endereço *MAC* do dispositivo ao registado no servidor. Deste modo pode identificar a que *VLAN* ela pertence. Por ultimo, o *Swich* actualiza a tabela de associação de *VLAN,* para que os dispositivos possam se comunicar uns com os outros, quando pertencendo ao mesmo segmento da mesma *VLAN*.

O mesmo processo descrito em cima pode ser explicado pela seguinte lógica por (Barros, 2007):

Todo e qualquer dispositivo conectado a uma rede, é identificado unicamente pelo endereço *MAC* da sua estação de origem, através da sua placa de rede (*NIC – Network Interface Cart*). O *Switch* consegue detectar o endereço *MAC* através da sua associação a cada *VLAN,* possibilitando ao administrador da rede de uma forma física, deslocar uma estação de trabalho de um local para outro. Contudo este não altera a lógica da rede. O mesmo descreve que a

topologia por endereço *MAC* é uma topologia baseada em utilizadores. Vistos que as *VLAN* reconhecem cada dispositivo através da sua placa de rede, podendo assim associar à *VLAN* a qual estes se encontra configurado.

Todos os processos transcritos nos textos acima podem provocar uma sobrecarga na rede, em caso de má configuração. Por isso esse tipo de topologia deve ser bem analisado antes da sua implementação.

Contudo (Cisco Systems Inc, 2003), identifica como uma desvantagem da associação de *VLAN* por endereços *MAC,* a necessidade de todos os utilizadores estarem configurados logo no início, numa *VLAN*. Mas depois da configuração manual, os utilizadores podem ser encaminhados de forma automática.

Depois da configuração seja feita pelo administrador da rede, o ponto fraco acima mencionado torna-se uma vantagem, pelo simples facto que a exigência de uma configuração prévia obrigatória impede aos utilizadores não autorizados de se conectarem à rede, representando assim um acréscimo à segurança e estabilidade da rede (Cisco Systems Inc, 2003).

A Tabela 6 mostra um exemplo de uma *VLAN* de topologia por endereço *MAC*

Endereço *MAC*	009096201A06	006525565A56	569859555B85
VLAN	1	2	2

Tabela 6 – Associação de endereço *MAC* para cada *VLAN*

Na Tabela 6 temos a relação entre o endereço *MAC* e a *VLAN* associada. Como podemos verificar o endereço *MAC* 009096201A06 encontra-se configurado para a *VLAN* 1, enquanto os endereços *MAC* 006525565A56 e 569859555B85 se encontram configurados para a *VLAN*2.

2.3 *VLAN* baseado em Protocolo – *Protocol-Based VLAN*

A *VLAN* baseado em protocolo siga a mesma lógica da *VLAN* baseada em endereço *MAC,* só que em vez de usar endereço *MAC,* permite criar segmentos de rede usando diferentes tipos de protocolo (Zacaron, 2007). Assim podemos associar todos os dispositivos que utilizam o mesmo protocolo dentro da rede.

As topologias baseado em endereço *MAC* e a topologia baseado em Protocolo, minimizam o trabalho do administrador de rede, visto que todos os registos se encontram na tabela de base de dados do servidor (Zacaron, 2007), então fica na responsabilidade do *switch* a actualização da sua tabela e associação ao *VLAN* correspondente a cada dispositivo.

Este tipo de topologia é ideal para redes que suportam múltiplas variedades de protocolos de rede, ou seja, podemos associar vários tipos de dispositivos do mesmo protocolo numa *VLAN*, de modo que a partilha de recursos torna-se compatível (Savi, 2005).

A Tabela 7 mostra um exemplo de uma *VLAN* baseado em topologia por Protocolo:

Protocolos	*TCP/IP*	*IPX*	*Apple Talk*
VLAN	2	1	3

Tabela 7 – Associação de Protocolo para cada *VLAN*

A Tabela 7 demostra a segmentação da rede via protocolos. Para o protocolo *TCP/IP* este se encontra no segmento da *VLAN* 2, para *IPX* se encontra no segmento da *VLAN* 1 e por último Apple *Talk* para o segmento da *VLAN* 3.

3 Tipos de *VLAN*

Para que as *VLAN* possam se comunicar mesmo utilizando equipamentos de fabricantes diferentes sem que o utilizador aperceba dessa diferença, tornou um *standard* baseado na norma IEEE 801.1Q (Barros 2007).

Entretanto existe duas formas distintas de associar *VLAN*, sendo as seguintes (Barros, 2007):

- Estática

As *VLAN* Estáticas pertencem há topologia baseada em portas. Um dispositivo conecta a uma determinada porta de um *Switch*, ela é associada ao número de *VLAN* a de que esta porta se encontra configurada (Madeira, 2006).

Ou seja, as *VLANs* Estáticas são técnicas de associação por porta. Ou seja algumas portas do *switch* são atribuídas de forma estática, ficando assim configuradas até que o administrador de rede os altera (Webb, 2003).

Em caso de alteração de postos, o administrador de rede, terá de modificar as novas alterações da rede, de forma manual e associar a porta á *VLAN* a qual o dispositivo pertence (Webb, 2003).

- Dinâmicas

As *VLANs* dinâmicas pertencem há topologia baseada em endereço *MAC* ou em topologia baseado em protocolos. Fica na responsabilidade do administrador da rede, fazer os registos de todos os endereços *MAC dos* dispositivos, ou dos protocolos a serem ussados primoriadamente (Madeira, 2006). De modo a poderem associar as *VLAN* correctamente, mesmo havendo mudança de posto.

As portas de um *switch* conseguem de forma automática associar a que *VLAN* cada dispositivo pertence (Barros, 2007). Por outras palavras, se um determinado dispositivos ao associar a uma *VLAN*, as configurações sobre o mesmo não altere, mesmo que haja mudança de postos. Isto é devido ao *switch* que não atribui à primeira a associação da *VLAN*, mas sim procura primeiro na base de dados do servidor, a configuração da associação do *VLAN* a qual pertence e por último actualiza a lista de todos os *switches* (Barros, 2007).

> Este método proporciona uma menor administração dentro do "*wiring closet*" principalmente quando um utilizador não autorizado for adicionado á rede, por outro lado, exige mais administração no que concerne á configuração da base de dados de um programa de gestão da *VLAN* para a manutenção dos dados correctos dos diferentes utilizadores da rede (Cisco Systems Inc, 2003)

4 Vantagens na implementação de uma *VLAN*

Já se descreveu o que são as *VLANs*, as suas topologias e tipos de *VLANs* existentes, mas contudo para entendermos melhores o impacto que as *VLAN* será demostrada algumas da sua vantagem na sua implementação.

"As *VLAN*s proporcionam um método de criação de redes lógicas independentes, que segmentam a rede global em pequenos domínios lógicos, suportados na mesma rede física." (Serpa, 2010). Por conseguinte, as *VLAN* não possuem limitações físicas permitindo aos administradores de redes criar domínios lógicos que podem expandir em um ou vários *Switches.*

Dada a essa flexibilidade permite a diversificação e elaboração de vários tipos de organização na rede, resultante a existência de uma grande diversidade de vantagens na utilização dessa tecnologia, das quais vamos salientar algumas mais principais (Serpa, 2010):

- **Controle do tráfego *broadcast***

As *VLAN* fazem uma melhor gestão dos *broadcast* e os *broadcast stroms*, visto que eles oferecem domínios de *broadcast* separados, tendo uma melhoria na rede e reduzindo o número de pacotes que nela circula (Barros, 2007). Isso quer dizer que, ao segmentar uma rede, esse passa a ter menos domínios de *broadcast*, diminuindo o número de dispositivos dentro de cada segmento e consequentemente diminuindo o número de pacotes internos que circulam na rede.

De uma forma resumida, os *broadcasts* das outras *VLAN* são filtrados pelos *switch*, reduzindo assim esses efeitos negativos (Véstias, 2005).

- **Aumento de nível de Segurança**

As *VLAN* concedem uma separação de domínios lógicos, tendo por referência os níveis de cada camada do modelo *OSI* (Serpa, 2010). Assim podem dificultar o acesso de possíveis atacantes que não fazem parte desse domínio lógico, visto que os tráfegos entre *VLAN* são filtrados pelo *router*.

Durante o processo de criação de *VLAN*, é de responsabilidade do administrador de rede, especificar a que porto pertence cada *VLAN* e que recursos se encontram disponíveis a esse porto (Véstias, 2005).

Cada *switch* pode ser configurado de forma a informar o administrador da rede de possíveis acessos a recursos não autorizados sempre que estes ocorrem, independentemente da topologia utilizada (Véstias, 2005). O mesmo pode ser reforçado usando *router* para gerir as restrições entre tramas de *VLAN* diferentes (Véstias, 2005).

- **Segmentação da rede**

A criação de *VLAN* pode ser baseada na própria estrutura organizacional da empresa. Por conseguinte, o administrador da rede consegue agrupar utilizadores pertencentes ao mesmo departamento ou grupo de trabalho, independente deles estarem no mesmo espaço físico ou não (Barros, 2007). Deste modo pode possibilitar assim uma segmentação lógica da rede.

Em determinadas organizações, alguns sectores devem pertencer a uma *VLAN* diferente das restantes. O propósito disso é proteger informações sigilosas, como é o caso do departamento financeiro (Haffermann, 2009).

- **Aumento de Performance**

A criação de domínios lógicos os domínios de *broadcats* fica limitada, tornando a transmissão de pacotes restringidas somente a cada domínio, salvo algumas excepções, evitando assim tráfego desnecessário (Serpa, 2010).

Por natureza, as redes segmentadas são as que tem mais performance nos dias de hoje, principalmente na redução do tamanho de domínios de colisão (Barros, 2007). Isto é devido ao agrupamento de utilizadores, separados logicamente por *VLAN*, produzem menos tráfego num segmento, consequentemente diminuição de domínios de colisão e reduzem assim a lentidão apresentado pelos *routers*, no encaminhamento de trafego (Barros, 2007).

- **Flexibilidade**

A estrutura lógica de uma *VLAN* é independente da estrutura física (Barros, 2007). Ou seja, em caso de alteração da estrutura física da rede, pode não houver alterações em nível lógico. Mesmo que estas alterações acontecem o número de passo para uma configuração lógica é muito menor do que uma configuração a nível física.

Um utilizador pode ser adicionado a uma *VLAN* independentemente da sua localização física. Tendo ele o acesso a todos os recursos pertencentes ao seu domínio de *VLAN* e o acesso negado aos que não pertencem, mesmo que os recursos estejam no mesmo espaço físico (Véstias, 2005).

- **Redução de tempo e custos**

A utilização de uma *VLAN* conduz a uma solução de criação e gestão de rede, com um custo inferior do que as redes tradicionais. Não há necessidade da existência de um *switch* para cada domínio de *broadcast*, e de várias configurações de interfaces de ligação do *router* para o *switch* (Véstias, 2005). Um só *switch* com *VLAN*, consegue suportar múltiplos domínios de *broadcats* e necessita só uma configuração de interface de ligação entre o *switch* e o *router* (Véstias, 2005).

O uso de *routers* dedicados pode resolver o problema de interconexão de redes locais. No entanto esse tipo de solução faz com que o preço seja algo a considerar, implicando um investimento muito alto nesses tipos de equipamentos (Haffermann, 2009). Enquanto isso, o uso de *switches* com *VLAN* tornaria a implementação com os mesmos ganhos do *router*, mas por um preço muito mais baixo (Haffermann, 2009). Ainda o mesmo tem configurações mais

simples, menor tempo na reconfiguração na deslocação de dispositivos, tendo que estes só ocorrem a nível de *software* (Véstias, 2005).

5 *VLAN* com Múltiplos *Switches*

Até nesse momento, já foi revisito as *VLANs*, os seus protocolos e as suas vantagens na sua implementação. Mas como é que os *switches* se comunicam uns com os outros sabendo que podem existir segmentos de redes diferentes para cada *VLAN*? Nesse subcapítulo será descrito as respostas para essa e outras questões.

Uma *VLAN* pode ser definida numa variedades de *switches*, e que estes processos de encaminhamentos de tramas são parecidos, como a de um só *switch*. Contudo apresentam problemas na necessidade de comunicar tramas de *VLAN* diferentes (Véstias, 2005).

Para resolução do problema de comunicação de tramas de *Switches* diferentes, há que existir um protocolo padrão que identifica cada trama, a que *VLAN* pertencem (Véstias, 2005).

Para melhor compreensão desse tipo de ligação existe dois tipos de ligação entre *switches* (Angelescu, 2010):

- **Ligação de acesso** – *acess links*

" (…) é uma ligação cujas interfaces respectivas fazem parte de uma única *VLAN*, designada *VLAN* nativa do porto." (Véstias, 2005). É o mesmo que dizer que as tramas que são transmitidas não contem informação sobre o VLAN a que pertencem. Originando assim uma interface padrão chamada "*VLAN* 1", onde todos os dispositivos ao conectaram as suas interfaces, usarão esta interface para transmissão das suas tramas.

- **Ligação Partilhada** – *trunk links*

Inicialmente as *VLANs* apresentaram certas anomalias na implementação através de rede desde do seu fabrico (Barros, 2007). É que cada fabricante utilizava técnicas diferentes de implementação de *VLAN*, tornando assim as configurações manuais de cada *switch* impossível em redes de grande porte.

Foi nesse contexto que teve necessidade de um novo tipo de ligação que superava todo esses tipos de problemas. Assim surgiu o "*VLAN Trunking*", que adiciona "*tags*" ou etiquetas especiais aos quadros para que estes podem identificar cada *VLAN* (Barros, 2007). Permitindo assim que haja um espaço de manobra dentro da rede de uma organização, criando vários *VLANs*.

A ligação Partilhada é uma ligação cujas interfaces fazem parte de várias *VLANs*, de modo a permitir a transmissão de trafego dos mesmos de forma simultânea, tendo como padrão o poder de transmitir tramas de todas as *VLANs* (Véstias, 2005). Contudo cabe ao administrador de rede, o poder de definir as restrições de cada grupo de *VLAN* nas ligações partilhadas (Véstias, 2005).

Existem três tipos possíveis de ligação partilha, sendo elas as seguintes (Véstias, 2005):

- **Ligação entre um *switch* e um servidor**

Podemos ligar um *switch* a um servidor usando ligações partilhadas, tendo assim um servidor pertencendo a dois ou mais domínios de *broadcast* (Véstias, 2005). Permitindo que os utilizadores pertencendo a um *VLAN*, associada a uma ligação partilhada, ter acesso ao servidor sem necessidade de um *router* (Angelescu, 2010).

Por outro lado, se o *switch* não suporta ligações partilhadas, o servidor deve ser inserido numa *VLAN* e usar um *router* para encaminhamento de o acesso dos utilizadores da outra *VLAN* (Angelescu, 2010).

- **Ligações entre dois *switches***

As ligações partilhadas não existam comunicações de tramas entre *switches*. Enquanto na ligação partilhada, a interface de comunicação de tramas é comum para todas as *VLAN* (Véstias, 2005).

- **Ligações entre *switch* e um *router***

Existe a necessidade de usar um só *router* com apenas uma interface ligada ao *switch* através de uma ligação partilhada. Deste mondo, permitindo que o *router* receber tramas de todas os *VLAN* numa única interface (Véstias, 2005).

Contudo, sem a existência de ligações partilhadas, o encaminhamento de tramas de diferentes *VLAN* ficava sob a responsabilidade do *router*, através de associação uma nova interface, tornando o mesmo processo a ter um preço elevado e pouca flexibilidade (Angelescu, 2010).

Apesar das suas vantagens na ligação de múltiplas *VLAN*, o mesmo pode tornar instável para rede se não houver um acompanhamento correcto das tramas dentro das suas *VLAN* (Véstias, 2005).

Para combater isso foi criada uma nova abordagem de rotulagem, conhecido por rotulagem de *VLAN* (*VLAN tagging*) ou por rotulagem de trama (*frame tagging*). O único objectivo desse

método é reconhecer o campo identificador de *VLAN*, que é designado por *ID* da *VLAN* ou cor da *VLAN* (Véstias, 2005).

Esse processo de rotulagem decora da seguinte forma (Angelescu, 2010):

- Para que uma *VLAN* envia uma trama usando linhas partilhadas, cabe primeiro ao *switch* acrescentar no cabeçalho, a identificação da *VLAN* e só depois pode transmitir a trama.
- Para que uma *VLAN* envia uma trama usando linha de acesso, o *switch* retira primeiro o cabeçalho com a identificação do *VLAN*. Contudo esse processo só decorre em trama vem de uma transmissão partilhada, como é do caso acima. Depois é reenviar a trama para o destino final.

6 Métodos de rotulagem de tramas

Como método de rotulagem de tramas, exista uma diversidade de protocolos das quais irá ser explicado cada um, de forma mais detalhados.

6.1 Ligação *Inter-Switch – ISL* ou *Inter Switch Link*

A ligação *Inter-Switch* é um "protocolo proprietário desenvolvido pela *Cisco*. É usado em interfaces *FastEthernet* e *GibabitEthernet*. O *ISL* pode ser usado na ligação entre *switches*, entre *switch* e um *router* e entre um *switch* e um servidor" (Véstias, 2005).

O *ISL* liga dois *switches Cisco,* percorrendo os quadros *Ethernet,* executando o "*etiquetas externas*" ou "*encapsulação*" das tramas, como são conhecidos (Barros, 2007).

O cabeçalho do *ISL* inclui vários campos, mas o mais importante é o campo *VLAN,* lugar onde se pode codificar o número de *VLAN* (Zacaron, 2007).

O protocolo *ISL* ao identificar um quadro com o número correcto da *VLAN* do cabeçalho, cabe ao *switch* remetente certificar-se que *switch* o receptor sabe identificar a que *VLAN,* o quadro encapsulado pertence (Zacaron, 2007). Contudo, quando é enviada a trama original pelo um dispositivo, encontra-se no cabeçalho do *ISL,* os endereços *MAC* dos *switches* remetente e o receptor.

O protocolo *ISL* é o método de identificação de tramas mais usado pela Cisco. A trama original é encapsulada com um cabeçalho *ISL* de 26 *bytes* e um bloco de sequência de verificação de trama (*FCS – Frame Check Sequence*) de 4 *bytes* no final da trama (Véstias, 2005). Devido a esse cabeçalho, a trama pode atingir um tamanho máximo de 1548 *bytes*, mas este só pode ser reconhecido por equipamentos que suportam *ISL*, normalmente equipamentos Cisco. A figura 5 mostra o encapsulamento de um trama através do protocolo *ISL*.

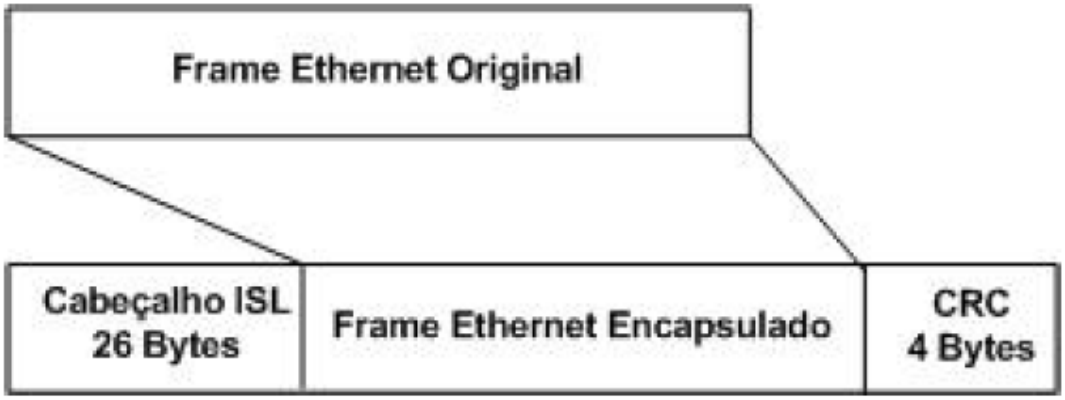


Figura 5 – Encapsulamento *ISL* da trama[1]

Fonte: adaptado de (Zacaron, 2007)

6.2 *IEEE 802.1Q*

O *IEEE 802.1Q* é um protocolo *standard* criado pela *IEEE*. Ela também como o do protocolo *ISL* é usada em interfaces *FastEthernet* e *GibabitEthernet*. A diferença é que, ela é usada quando pretendemos interligar equipamentos de fabricantes diferentes (Véstias, 2005). Um exemplo bem claro é a ligação de um *switch Cisco* com outro *switch* de outro fabricante. Também insere um campo na trama para poder identificar a *VLAN*.

O protocolo *IEEE 802.1Q* identifica quadros com o número de *VLAN*, usando um estilo de cabeçalho diferente do protocolo *ISL*. O protocolo *IEEE 802.1Q* simplesmente adiciona um cabeçalho de 4 *bytes* ao cabeçalho *Ethernet* original, que serve de identificador campo da *VLAN* (Zacaron, 2007). Contudo é necessário um novo cálculo de campo *FCS* original no *Trailer Ethernet*, porque o *FCS* é baseado no conteúdo do quadro inteiro (Zacaron, 2007).

O mesmo pode ser visito na figura 6:

[1] Disponível em: http://www2.dc.uel.br/nourau/document/?down=562 consultado em 02/08/2010

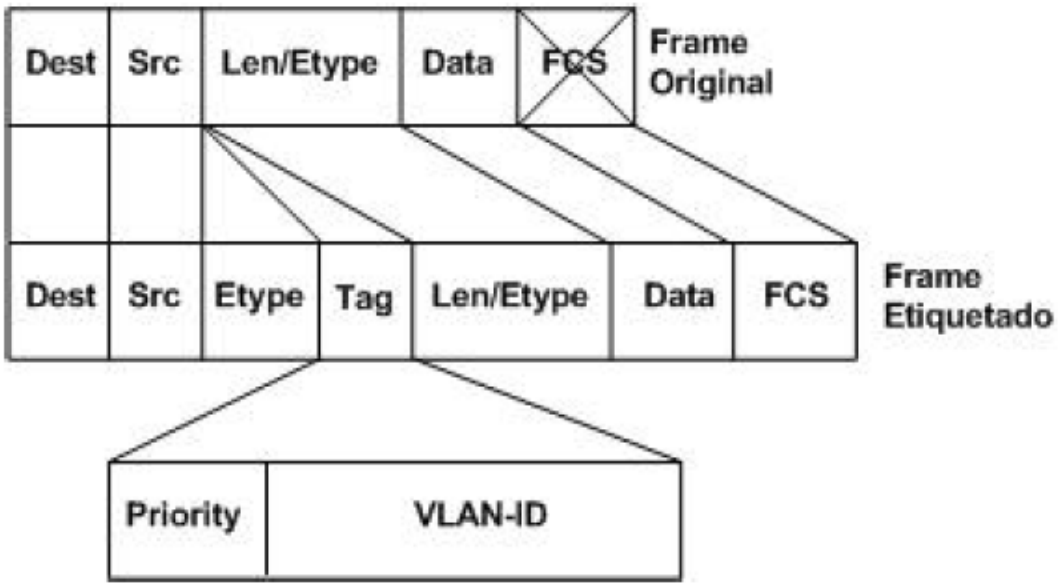


Figura 6 – Encapsulamento *IEEE 802.1Q* da trama[2]
Fonte: adaptado de (Zacaron, 2007)

6.3 *IEEE 802.10*

O protocolo *IEEE 802.10* é um protocolo *standard* criado pelo *IEEE*. É usado em interfaces *FDDI* (Véstias, 2005).

O protocolo *IEEE 802.10* é também um método seguro de transição de dados através de *backbone,* definindo um tipo único quadro chamado *SDE (Secure Data Exchange)* (Cisco, 2010).

6.4 Emulação LAN- LANE ou LAN Emulation

A emulação *LAN* é um protocolo que usa um método de encapsulamento para interligar *switches* através de uma rede ATM. Por conseguinte, em vez de identificar explicitamente a trama, ela utiliza uma ligação virtual entre os *switches* para cada *VLAN* (Véstias, 2005). Tornando assim que a identificação de cada *VLAN* seja implícita nas ligações Virtuais.

[2] Disponível em: http://www2.dc.uel.br/nourau/document/?down=562 consultado em 02/08/2010

7 Protocolo de Configuração e Manutenção de *VLAN-VTP*

Antes de o protocolo *VTP* seja descrito, será feita uma análise há seguinte situação. Para actualizar os parâmetros nos *switches*, teríamos de fazer a actualização de forma manual entre todos os *switches.* Isso podia tornar-se numa tarefa um pouco complicada, se for numa rede de dimensões grandes. Então surgiu a necessidade de todo esse processo seja feito de forma automático ou centralizado, garantido que qualquer alteração nos parâmetros seja reconhecido entre todos os dispositivos.

O *VTP (VLAN – Trunking Protocol)* é um protocolo proprietário da *Cisco*, criado a fim de resolver o problema acima referido (Guilherme, 2009).

O protocolo *VTP* faz a gestão de *VLAN* dinamicamente, permitindo assim que o administrador de rede consegue adicionar/remover ou alterar a configuração de *VLAN* em qualquer *Switch*, desde que pertençam ao mesmo domínio e tenham ligação partilhada (Véstias, 2005).

7.1 Funcionamento do Protocolo *VTP*

Para uma boa gestão dinâmica de *VLAN* baseado no protocolo *VTP,* cabe ao administrador de rede começar primeiro a criação de um domínio *VTP* e determinar quais os *switches* que pertencem ao domínio (Véstias, 2005).

O administrador de rede deve escolher um *switch* para ser o servidor *VTP* do domínio e que os restantes *switches* ficam cliente ou em modo transparente. A cada 5 minutos, o protocolo *TVP* envia informação de gestão, ou o mesmo é alterado a cada vez que o administrador altera a configuração de *VLAN* (Véstias, 2005). Nessa informação vem contido informações de gestão do *VTP,* o número de revisão da configuração, os números e nomes das *VLAN* e por último a lista de *VLAN* usadas em cada um dos *switches* da rede. O número de revisão de configuração é incrementado sempre que o servidor *VTP* altera a informação de *VLAN* anunciada aos restantes *switches* (Angelescu, 2010).

Os *switches* podem operar em três modos diferentes, sejam eles os seguintes (Guilherme, 2009):

- ***VTP* modo Servidor – *VTP Sever mode***

Todos os *switches Cisco* vêm configurados como *VTP* Servidor, por defeito. Toda informação se encontra armazenada localmente, em um *NVRAN* separada onde o *"startup-config"* está armazenado (Guilherme, 2009). Qualquer registo de alteração realizado no servidor *VTP* será replicado automaticamente para todos os outros *switches* pertencentes ao mesmo domínio *VTP* (Guilherme, 2009). O servidor *VTP* pode criar, modificar e apagar VLAN. Estas operações só podem ser realizadas em ligações partilhadas, aos restantes *switches* do domínio que operem em modo cliente (Véstias, 2005).

- ***VTP* modo Cliente – *VTP Client mode***

O *VTP* em modo Cliente, torna o *switch* num dispositivo que só recebe e envia anúncios pelas linhas partilhadas. Mas os mesmos não podem criar, alterar ou apagar *VLAN* (Véstias, 2005). Todas as informações armazenadas em sua memória *RAM*, no entanto essas informações são guardadas em *NVRAM*. Por isso quando um *switch* for desligado não perde as configurações sobre as *VLANs* (Guilherme, 2009).

- ***VTP* modo Transpatente – *VTP Transparent mode***

O *VTP* modo Transparente é um "meio-termo" que fica entre o *VTP* modo servidor e um Cliente. Contudo o mesmo não participa no domínio *VTP* (Guilherme, 2009).

O modo transparente é quando o administrador não quer que um *switch* obedeça aos anúncios *VTP* de configuração de *VLAN* do servidor *VTP*, mas que este propaga os anúncios *VTP* ao longo do seu domínio (Véstias, 2005).

Um *switch* em modo transparente pode criar, modificar ou apagar a sua informação de *VLAN*, mas essa informação não é propagada aos outros *switches* do seu domínio (Véstias, 2005).

8 Considerações finais

No capítulo da *VLAN* foi elaborado vários assuntos sobre a *VLAN*, desde da sua definição, tipos de *VLANs*, topologias da *VLANs*, vantagens em uso da *VLAN* entre outros.

As *VLANs* apresentam como tecnologia para monotorização e gestão da rede, bem eficaz e de uma forma simples. Os seus protocolos de ligação de tramas são bastantes simples, mas contudo apresentam um grande grau de conhecimento. Pelo facto de este ser gerenciado e monitorizado, ela torna uma ferramenta de extrema importância para qualquer administrador da rede. O uso dessa tecnologia e os seus protocolos representa um acréscimo a segurança, estabilidade da *LAN* nas organizações, facilitando assim a tarefa ao administrador da rede.

De uma forma resumida, o uso das *VLANs* na rede das Organizações vem trazer mais eficácia e performance à rede. Ainda vem com um conjunto de Vantagens, e mecanismos de gestão e monotorização da rede, bastantes simples e eficaz para os administradores da rede.

Capítulo 3: O Caso da UniPiaget

1 A Entidade Instituidora

O instituto Piaget é uma instituição cooperativa para o desenvolvimento humano integral e ecológica, sem fins lucrativos, que se obriga, pelos seus estatutos, a reinvestir todos os excedentes resultantes da sua actividade.

Criado em 1979 pelo Presidente institucional, Director de investigação e líder da comissão, Prof. António de Oliveira Cruz, com inteira aceitação do seu patrono Jean Piaget. O instituto Piaget é uma cooperativa para o Desenvolvimento Humano integral e Ecológico. O instituto vem desenvolvendo a sua actividade desde há 29 anos. [3]

Ao longo desse tempo de actividades, o instituto Piaget vem vindo a inserir-se em diversas regiões, normalmente apartado das grandes cidades, criando Universidades como em Angola, Cabo verde e Moçambique.

2 Universidade Jean Piaget de Cabo Verde

A Universidade Jean Piaget de Cabo Verde é um estabelecimento de ensino superior, criado pelo instituto Piaget, e tem como missão contribuir para a alta qualidade de formação dos recursos humanos em Cabo Verde, bem como para o desenvolvimento de competências locais

[3] Disponível em http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=1 consultado em 12/07/2010

imprescindíveis para o desenvolvimento do país e de modo a clarificaram cada vez o nome da instituição.

No dia 7 de Maio de 2001, a universidade inicio a suas actividades com a abertura do 1º ano do curso de Sociologia, como um estabelecimento de ensino superior de interesse publico, reconhecido pelo decreto-lei nº 12/2001.[4]

Segundo (Mendes, 2009), a UniPiaget goza de autonomia de gestão, científica, pedagógica e cultural. Ela exerce a sua actividade sem prejuízo das responsabilidades e projecto da Entidade Instituidora, em paralelo com as Universidade oficiais, às quais se encontra legalmente enquadrada no sistema nacional de educação. A Universidade Jean Piaget tem como meta, a cooperativa para o desenvolvimento humano, integral e ecológico, instituição com fins de utilidade pública e de solidariedade social e sem fins lucrativos. Sendo ela totalmente privada, é dirigida por um administrador Geral, que represente o Instituto Piaget, e pelo Reitor, responsável pela gestão da Universidade nos domínios científicos e pedagógico.

3 Organização

A UniPiaget é constituída por uma estrutura académica e administrativa. Sujeito a um sistema misto de governo, esse reúne as responsabilidades que decorrem dos estatutos de cada instância. Os órgãos colegiais e órgãos individuais fazem parte do órgão de governo.[5]

A organização é apresentada pela seguinte lógica:

- **Órgãos do Governo**
  - **Órgãos individualistas da Universidade**
    - ✓ Administrador Geral
    - ✓ Reitor
  - **Órgãos colegiais da Universidade**
    - ✓ Conselho Consultivo – Presidido pelo Administrador Geral
    - ✓ Conselho Geral – Presidido pelo Reitor
    - ✓ Conselho Científico

[4] Disponível em http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=1 consultado em 12/07/2010
[5] Disponível em http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=3 consultado em 13/07/2010

- ✓ Conselho Pedagógico
- ✓ Conselho Disciplinar

- **Organização científica e Pedagógica**[6]
  - ➢ Comissões Científicas
  - ➢ Comissões de Cursos
- **Unidades Organizacionais**[7]
  - ➢ Serviços de Documentação – SD
  - ➢ Serviços Administrativos e Auxiliares – SAA
  - ➢ Serviços Financeiros e Sociais – SFS
  - ➢ Secretariado Executivo – SE
    - ✓ Administração
    - ✓ Reitoria e Órgãos Colegiais
  - ➢ Gabinete de Estudos e Planeamento – GEP
  - ➢ Gabinete de Formação Permanente – GFP
  - ➢ Gabinete de Comunicação e imagem – GCI
  - ➢ Departamento de intercâmbio e formação Avançada – DIFA
  - ➢ Divisão Tecnológica - DT

O mesmo é demonstrado na figura abaixo (Figura 6).

[6] Disponível em http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=4 consultado em 13/07/2010
[7] Disponível em http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=5 consultado em 13/07/2010

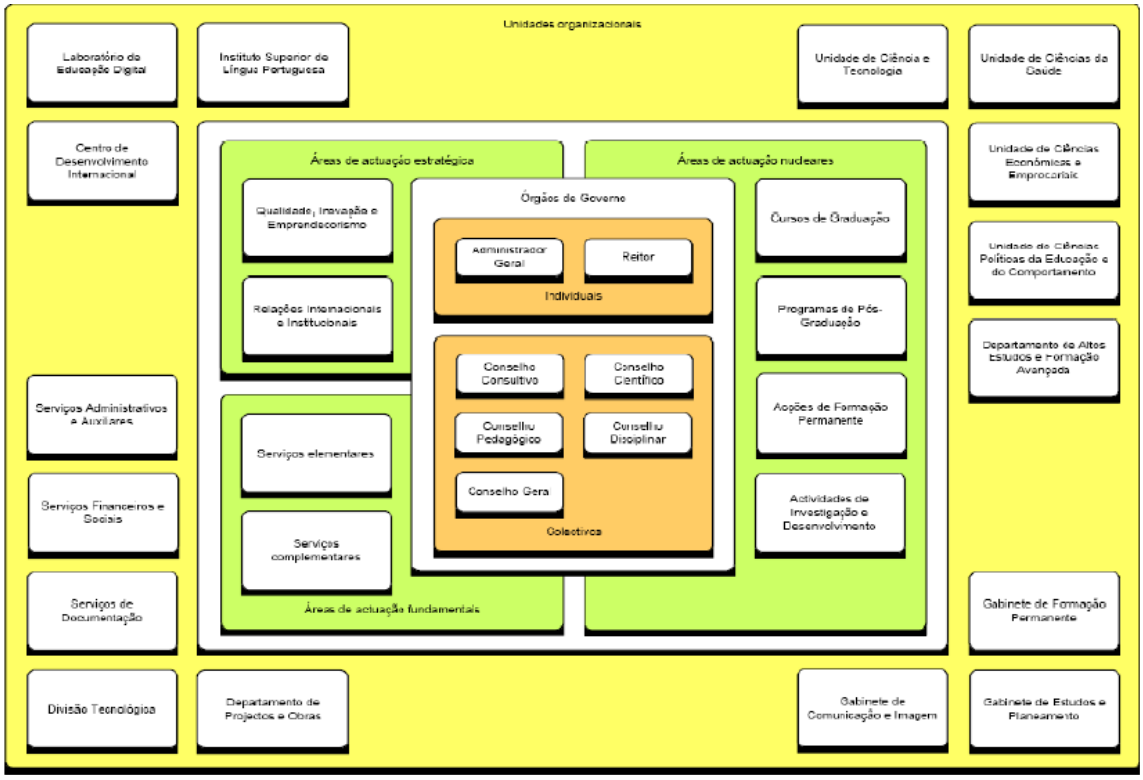


Figura 7 – Estrutura e organização de UniPiaget

Fonte: adaptado de Pereira (2007)

4 Divisão tecnológica

A Divisão Tecnológica da Universidade Jean Piaget de Cabo Verde como unidade Organizacional responsável por toda a Tecnologia de Informação e Comunicação, tem como missão prover à instituição os recursos e serviços das Tecnologias de Informação e Comunicação de modo a optimizar o desempenha da organização, de uma forma profissional e como grande grau da qualidade e rapidez.

Segundo (Mendes, 2009) no ano lectivo 2001/02, a Divisão Tecnológica arrancou as suas actividades. Ela era supervisionada por um coordenador, que assumia toda a parte técnica e operacional. Depois foram recrutados dois estagiários, mas com aumento da demanda de serviços contratou-se um técnico, e ficando os estagiários a trabalhar exclusivamente nos laboratórios de informática. Como o técnico e os estagiários tiveram grandes constrangimentos, desde de computadores obsoletos, deficiência sistema de abastecimento de electricidade, falta de servidores, rede estruturada não documentada e entre n situações.

Ainda (Mendes, 2009) descreve que decorridos oito anos, Divisão tecnologica é uma direcção que funciona como delegação autónoma de Cabo Verde, tendo três secções distintas (1

Director, 3 funcionários, 3 prestador de serviços, um estagiário), sendo o mesmo reponsável pela gestão de mais 200 postos de trabalhos, 14 servidores, 24 impressoras e mais de 1500 utilizadores no campus Univerisitário da cidade da Pria e no pólo Universitário do Mindelo

4.1 Organização Interna

A Divisão Tecnológica é constituída em três secções distintas[8], sendo elas as seguintes:

- Suporte – garante assistência técnica aos utilizadores;
- Desenvolvimento – responsável pelos *softwares* de gestão e pelo desenvolvimento de pequenas aplicações;
- Sistema – garante o funcionamento normal dos servidores e da rede multimédia da Universidade.

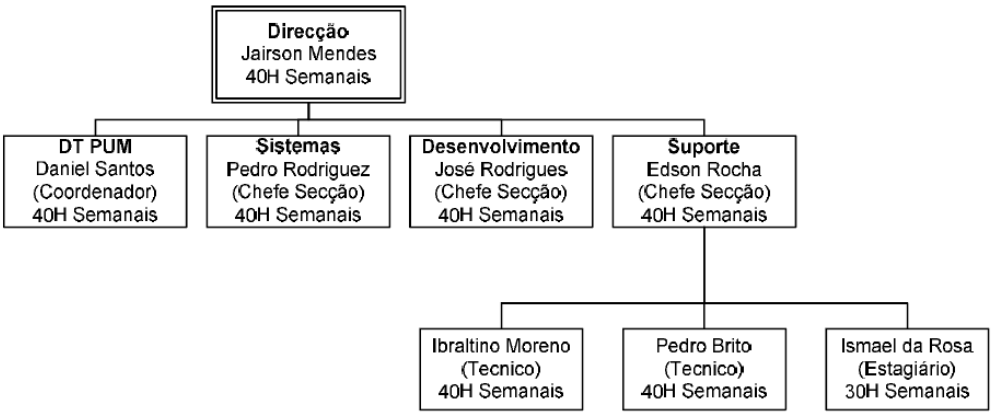


Figura 8 – Estrutura organizacional da Divisão Tecnológica

Fonte: adaptado de (Mendes, 2009)

5 Proposta de uma *VLAN*

A rede que se apresenta, pretende contribuir com mais uma tecnologia de trabalho para gestão, monotorização e manutenção da rede da Universidade Jean Piaget de Cabo Verde. O mesmo é destinado aos administradores da rede da universidade, levando os mesmos a atingir um grande nível de segurança e estabilidade da rede. Foi feito um levantamento de requisitos dentro da Instituição em causa, de modo que a proposta de *VLAN* seja a mais realista de acordo as necessidades exigidas.

Dentro desse levantamento foi recolhido informações suficientes para elaboração de um perfil da rede, que ajusta as necessidades da rede universitária. A partir desse perfil será elaborado os perfis das *VLANs* e o desenho da rede pretendida para a Instituição.

5.1 Levantamento de requisitos

Devido a alguns constrangimentos causados pela rede actual, optou-se pela apresentação de uma proposta de uma nova infra-estruturação da rede da Universidade, onde a mesma é separado por domínios lógicos através do uso da *VLAN*. A proposta leva em conta a necessidade de gestão da rede, a sua manutenção e monotorização, de uma forma simples e eficaz de modo a dar resposta às necessidades da universidade. Por outras palavras, o uso da *VLAN* na UniPiaget vai aumentar a eficácia e eficiência da rede universitária. Deste modo a rede desenhada aproxima mais da rede pretendida de acordo com as necessidades da Universidade.

De acordo com os dados recolhidos em terreno da universidade foi elaborado uma tabela que descreve a distribuição de cada sector da universidade, assim como os seus níveis de importância, como em que domínios podem ser inseridos. Os dados da importância e do domínio são numéricos de modo a prevalecer o sigilo dentro da organização. Cabe ainda salientar que os números dentro de importância varia de 1 (menos importância) até 5 (alta importância) como e descrito na tabela abaixo. A primeira tabela descreve o bloco A, desde das salas de aulas, como nos gabinetes existentes na universidade (Tabela 9).

Sala	Sigla	Importância	Domínio	Bloco
A101	SAA / RH	3 e 4	3 e 4	A
A102	Não Tem	2	3	A
A103	Lab Física	1	1	A
A105	Não Tem	1	6	A
A107	Lab Química	1	1	A
A108	Lab Biologia	1	1	A
A110	Não Tem	3	4	A
A113	Bar	3	4	A
A119	CDE	2	3	A
A201	SFS	3	4	A
A202	Não Tem	3	2	A
A203	GEP	3	2	A
A204	Não Tem	2	2	A

[8] Disponível em http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=5 consultado em 13/07/2010

A205	Lab Informática	2	1	A
A206	Lab Informática	2	1	A
A210	Lab cv móvel	2	1	A
A211	Lab interatlântico	2	1	A
A214	AG	4	5	A
A215	SE	3	3	A
A216	R	4	5	A
A217	SR	1	6	A
A218	SD	3	1 e 3	A

Tabela 8 – Descrição do Bloca A

Depois temos a descrição do bloco B (Tabela 10)

Sala	Sigla	Importância	Domínio	Bloco
B101	Não Tem	1	1	B
B102	Não Tem	1	1	B
B103	Não Tem	1	1	B
B104	Lab Fisioterapia 1	1	1	B
B105	Lab Fisioterapia 2	1	1	B
B110	Não Tem	1	1	B
B111	Não Tem	3	4	B
B112	Lab Imprensa	2	1	B
B113	Lab Rádio	2	1	B
B114/ B115	Anfiteatro	1	6	B
B116/ B117	Anfiteatro	1	6	B
B122	Lab televisão	2	1	B
B201	Não Tem	1	1	B
B202	Não Tem	1	1	B
B203	Não Tem	1	1	B
B204	Lab Arquitectura	2	1	B
B205	Não Tem	1	1	B
B210	Não Tem	1	1	B
B211	Não Tem	2	2	B
B212	LED	4	5	B
B213	Lab Informática	2	1	B
B214	Não Tem	2	1	B
B215	Lab Imprensa	2	1	B
B216	DT	5	5	B
B217	Não Tem	1	1	B
B218	Não Tem	1	1	B
B219	Não Tem	1	1	B
B220	Não Tem	1	1	B

Tabela 9 – Descrição do Bloca B

5.2 Perfil da Rede

Como foi referido no capítulo 2, a rede *VLAN* pode ser criada de acordo com a necessidade da Organização, por isso a escolha de melhor perfil pode determinar o sucesso ou fracasso da rede, bem como a metodologia a seguir.

Contudo a escolha de perfil pode depender dos recursos disponíveis, e da disponibilidade da organização em investir, de modo a não ultrapassar a realidade em que se encontra.

Nesse momento a Universidade tem disponível *Switch Catalyst 2960 series*. Esse equipamento tem 24 porta *FastEthernet* e 2 portas de *GigaFastEthernet*, e suporta a tecnologia de *VLAN*.

No caso da Universidade Jean Piaget, para a escolha do melhor perfil estes têm de responder a necessidade dos seguintes requisitos:

- Acesso a recursos na rede

O acesso a recursos na rede serve para identificar os recursos da rede, bem como quem tem acesso a esses recursos. São considerados recurso todos os dispositivos finais da rede (impressora, fax, etc.) e serviços prestados pela organização (internet, vídeo conferencia, etc.).

- Acesso a Servidores

Para identificar a que tipo de perfil tem acesso a que parte ou totalidade dos servidores. Com isso podemos filtrar qualquer acesso a um servidor que não pertence a esse segmento de rede, bem como acesso a partilhas.

- Aplicações e *softwares* de Gestão

Numa segmentação da rede fica somente as aplicações e *Softwares* de gestão, como é o caso do ERP *"Primavera Business Software Solution"*, onde a circulação de dados na rede é sigilosa e confidencial.

Levando em conta todos esses requisitos, foram identificados 6 tipos distintos de perfil, sendo eles descritos pela seguinte forma.

1. *Vlan1* - Alunos

Como o nome descreve esta *Vlan* e designado especialmente para os alunos. O mesmo pode ser usado em outras circunstâncias, como é o caso de formações e seminários. A *Vlan1* Alunos tem como características o acesso só aos computadores e servidor de autenticação (onde se encontra inseridos as suas contas de perfil), e negado acesso a outras equipamentos como impressoras e outros servidores. Ainda o mesmo suporta a infra-estrutura de rede sem fios (*wireless* – nome qual é designado em inglês). Entre os seis tipos de perfil é o que mais dispositivos contêm.

As tabelas seguintes descrevem os departamentos/salas que pertencem a Vlan1, sendo a maioria pertencendo ao bloco B, sendo entre eles salas de aulas e laboratórios. Primeiro vamos ver o Bloco A (Tabela 11) e de seguida do Bloco B (Tabela 12) respectivamente.

Nome	Sala	Bloco
Lab Física	A103	A
Lab Química	A107	A
Lab Biologia	A108	A
Lab informática	A205	A
Lab informática	A206	A
Sala CV móvel	A210	A
Sala interatlântico	A211	A
Mediateca	A218	A

Tabela 10 – Descrição da *VLAN1* – Alunos do Bloco A

Nome	Sala	Bloco
Sala de aula	B101	B
Sala de aula	B102	B
Sala de aula	B103	B
Lab Fisioterapia 1	B104	B
Lab Fisioterapia 2	B105	B
Sala de aula	B110	B
Lab imprensa	B112	B
Lab Rádio	B113	B
Anfiteatro 1	B114/B115	B
Anfiteatro 2	B116/B117	B
Lab televisão	B122	B
Sala de aula	B201	B
Sala de aula	B202	B
Sala de aula	B203	B
Lab Arquitectura	B204	B
Sala de aula	B205	B

Sala de aula	B210	B
Lab informática	B213	B
Sala de aula	B214	B
Lab imprensa	B215	B
Divião tecnológica	B216	B
Sala de aula	B217	B
Sala de aula	B218	B
Sala de aula	B219	B
Sala de aula	B220	B

Tabela 11 – Descrição da *VLAN1* – Alunos do Bloco B

Em nível de infra-estrutura a rede da *VLAN1* – Alunos é descrevida da forma como é demonstrada na Figura 9.

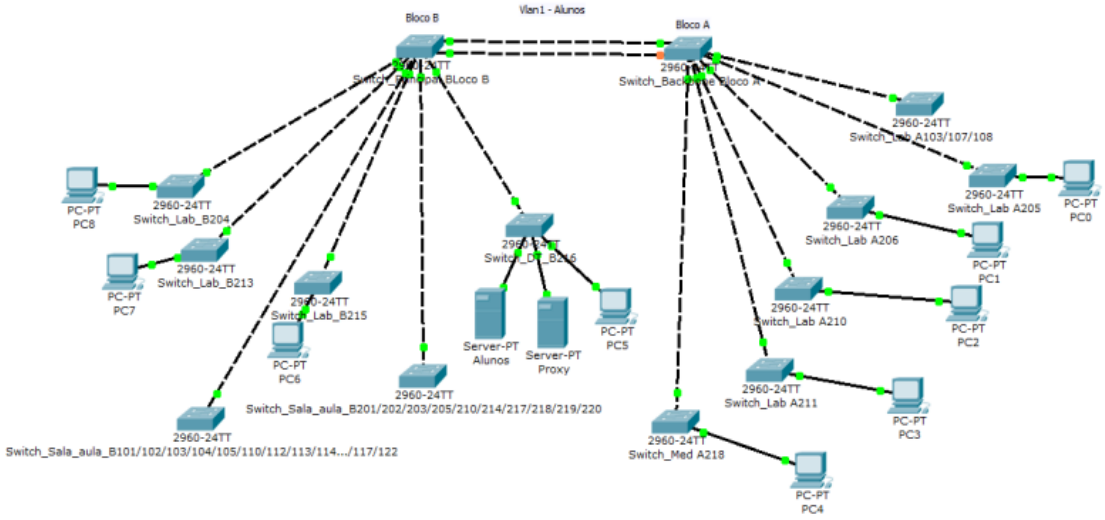


Figura 9 – Infra-estrutura da *VLAN1* – Alunos

2. *VLAN2* – Docentes

A *VLAN2*, tendo em conta a *VLAN1*, não é uma rede dedicada somente aos docentes da universidade, mas também para alguns funcionários que trabalham com os docentes. É caso das Unidades que têm ainda acesso a impressoras e a servidor de autenticação. A *Vlan2* apresenta mais características do que a *VLAN1*, contudo o número de departamentos e de utilizadores é muito menor. Uma das principais características dessa segmentação lógica é que ela está quase totalmente presente no Bloco A.

A tabela seguinte demostra os departamentos da *VLAN2* (Tabela 13).

Nome	Sala	Bloco
Unidades	A202	A
Gabinete de Estudos e Planeamento	A203	A
Sala de Docentes	A204	A
Sala de Docentes	B211	B

Tabela 12 – Descrição da *VLAN*2 – Docentes

Em nível de infra-estruturação a rede fica representada da seguinte forma, ver Figura 10:

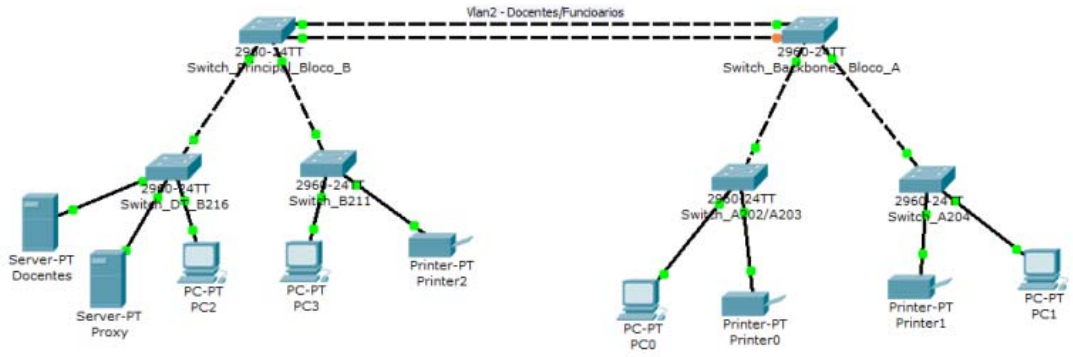


Figura 10 – Infra-estrutura da *VLAN2* – Docentes

3. *VLAN3* – Funcionários

A *vlan3* é a *VLAN* destinados aos funcionários, que tem postos de trabalhos fixos e com equipamentos. Contudo não fazem parte dela os funcionários que trabalham com a aplicação "*Primavera Business Software Solution*". Como as das outras segmentações tem acesso a um servidor de autenticação e acesso a impressoras. Uma das principais características da *VLAN3* é que ela situa-se completamentos no Bloco A.

A mesma é representada pela Tabela 14.

Nome	Sala	Estado	Bloco
Serviços administrativos e Auxiliares	A101	1	A
Telefonista	A102	1	A
Centro Desenvolvimento Empresarial	A119	1	A
Serviços Executivos	A215	1	A
Mediateca, Serviço de documentação	A218	1	A

Tabela 13 – Descrição da *VLAN3* – Funcionários

A mesma é descrita pela seguinte infra-estrutura (ver Figura 11).

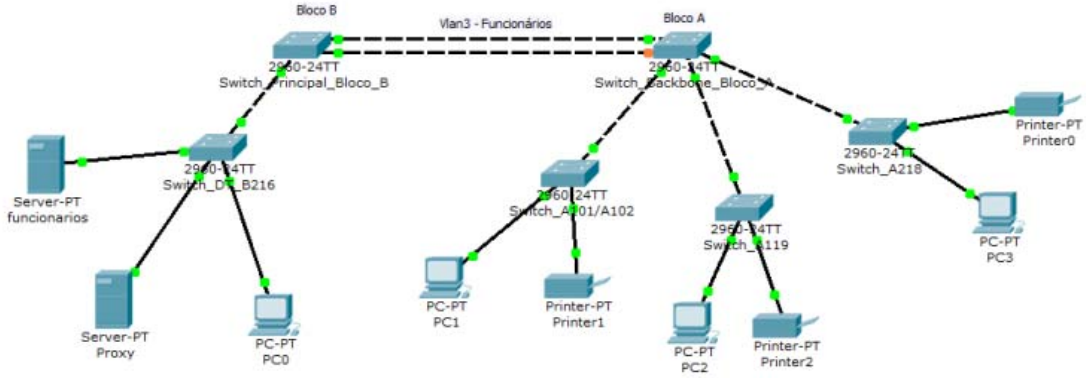


Figura 11 – Infra-estrutura da *VLAN3* – Funcionários

4. *VLAN4* – Primavera

A *VLAN4* é descrita como a *VLAN* reservada exclusiva especialmente à aplicação ERP "*Primavera Business Software Solution*", de modo a garantir o sigilo e confidencialidade dos dados. Desta forma torna-se mais segura e rápida a transferências de dados, devido a dimensão da segmentação da rede e de números de recursos finais presentes nesta segmentação. Em relação a outras segmentações, esta tem acesso também a um servidor de autenticação, a um servidor de Aplicações e acesso a impressoras. Esta presente quase totalmente no bloco A. A *VLAN4* pode ser representada pela Tabela 15.

Nome	Sala	Estado	Bloco
Serviço Administrativos e Auxiliares	A101	1	A
Tesouraria	A110	1	A
Bar e Refeitório	A113	1	A
Serviço Financeiro e Social	A201	1	A
Reprografia	B112	1	B

Tabela 14 – Descrição da *VLAN4* – Primavera

E pela seguinte infra-estrutura, ver Figura 12.

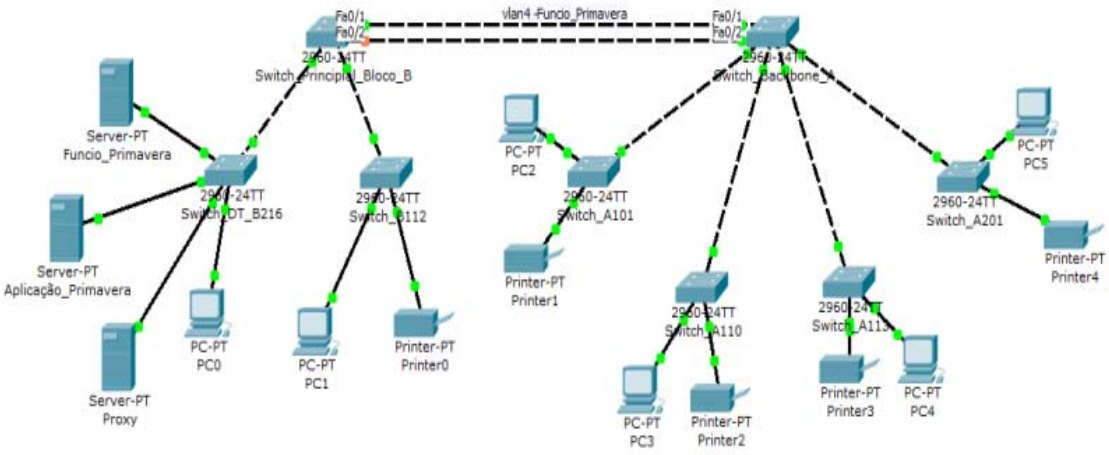


Figura 12 – Infra-estrutura da *VLAN*4 – Primavera

5. *VLAN5* – Permissões Especiais

A *VLAN5* é a única *VLAN* com capacidade de mudar de uma segmentação para outra e ter acesso a todos os recursos da rede. Mas isto só é possível através de um *router*. A *VLAN5* é descrita como *VLAN* administrativa, de onde pode ter acesso a qualquer dispositivo na rede. Nela desencadeia-se todos os processos desde manutenção e configuração das *VLAN*, bem como a sua monotorização. Pertence a esse tipo de *VLAN* só responsáveis da organização e o administrador de rede, salvo pequenas excepções.

Tudo isso pode ser demonstrado na Tabela 16.

Nome	Sala	Estado	Bloco
Administrador Geral	A214	1	A
Reitoria	A216	1	A
Laboratório de Ensino á Distancia	B212	1	B
Divisão tecnológica	B216	1	B

Tabela 15 – Descrição da *VLAN5* – Permissões Especiais

No nível de infra-estrutura, ver Figura 13

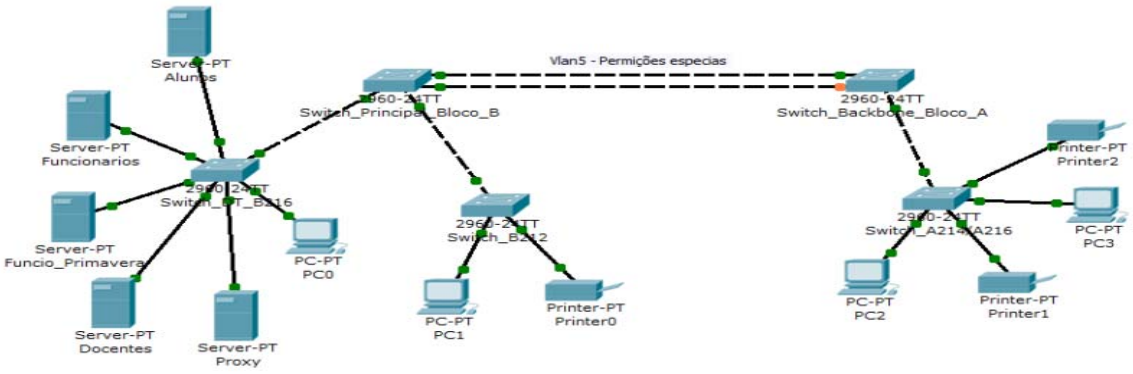


Figura 13 – Infra-estrutura da *VLAN5* – Permissões Especiais

6. *VLAN6* – Serviços Especiais

A *VLAN6* é a *VLAN* com menos privilégios de todos. Ela é feita especialmente para ser usada em certa circunstância, como em caso de formações profissionais. A mesma pode ser substituída pela *VLAN1* de modo que os utilizadores podem ter acesso a recursos, como é o caso de servidores. O que diferencia a *VLAN1* da *VLAN6* é que na *VLAN*1 a Organização está a oferecer o espaço geográfico como também serviços (servidor de autenticação, internet, etc). No entanto estes serviços podem ser prestados por outras organizações e não a própria universidade. De modo a não mudar a estruturação da rede universitária, a organização externa usa a *VLAN6*, assim desse modo todo ou qualquer serviço prestado fica disponibilidade somente para a segmentação da *VLAN6*, trato a excepção a *VLAN5*, que tem acesso a qualquer segmento da rede.

A *VLAN6* é representada pela seguinte Tabela 17.

Nome	Sala	Estado	Bloco
Auditório	A105	2	A
Sala de Reunião	A217	2	A
Antiteatro	B114 / B115	2	B
Antiteatro	B116 / B117	2	B

Tabela 16 – Descrição da *VLAN6* – Serviços Especiais

O mesmo apresenta a seguinte infra-estrutura, ver Figura 14

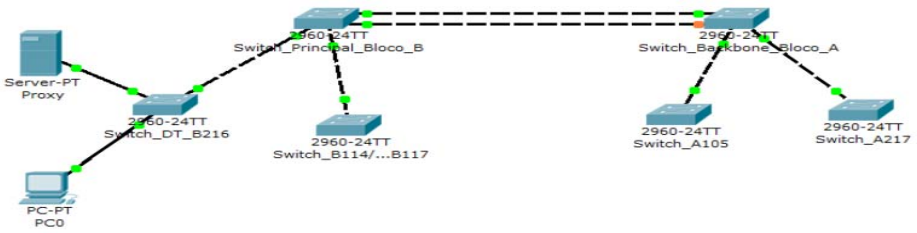


Figura 14 – Infra-estrutura da *VLAN6* – Serviços Especiais

5.3 *VLAN* na UniPiaget

Como visto nos perfil da rede (capitulo 5.2), a rede universitária pode ser segmentada em 6 segmentos, sendo um deles de administradores (permitindo a comunicação entre outros segmentos). A segmentação pode facilitar muito na comunicação e segurança numa rede, bem como estabilidade da rede em caso de falhas ou até quedas de algum segmento.

Este tipo de tecnologia vem como mecanismo de suporte e sustentabilidade da rede, reintegrando sem muito problema com outros mecanismos, e dando uma grande avalia na performance da rede. Esse tipo de respostas pode diferenciar uma rede bem estruturada, de uma funcional, permitindo com maior exactidão identificar a origem do problema.

O perfil da rede descrito no capítulo 5.2 serve tanto para *VLANs* estatísticas ou dinâmicas, representado o segmento da rede que cada *VLAN* deve pertencer. Cabe ainda salientar que no caso do *VLAN* dinâmica, esta tem de ser baseado em *MAC adrress* e a autenticação dos utilizadores deve ser feito através de um servidor de autenticação. Partir dos dados de tipo de utilizador, podemos designar a que *VLAN* este se encontra associado. De uma forma resumida, o perfil da rede elaborado nesse trabalho científico, é independe ta topologia escolhida, mas a designação das infra-estruturas escolhidas é da topologia baseado em porta.

A topologia baseada em portas é nesse momento o que mais adapta a realidade da Instituição em causa. Isto é devido relativamente ao preço, mais acessível, e dos recursos disponíveis, sabendo que a universidade tem nesse momento na sua posse, *Switches Catalist 2960*, que suportam *VLAN* baseada em portas.

Com a análise dos requisitos podemos identificar e documentar os *switches*, bem como as salas/departamentos. Tendo em conta que no momento existem dois Blocos (A e B), é recomendável que existam dois *switches* principais e que estes sejam a única ligação entre os dois Blocos e os outros 18 *Switch* para ligação geral da rede.

Visto que o *Switch* do Bloco B é que se encontra na Divisão Tecnológica, nela se encontrará configurado o Protocolo *VTP* em modo "*Server"* de modo a monotorização e criação das *VLANs* de forma automático. Cada um desses *Switch* terá um endereço *IP* na *Vlan native*, de modo a poder aceder esses por via "*Telnet"* e/ou "Browser" através do protocolo http (*Hypertext Transfer Protocol* ou em português Protocolo de Transferência de Hipertexto) ou https (*HypertTest Transfer Protocol Secure*), dependente da configuração inicial feito pelo utilizador.

Para uma melhor identificação do *switches* o mesmo é descrito nas seguintes tabelas, Tabela 18 e Tabela 19.

A Tabela 18 e a Tabela 19 se subdividam em 4 secções distintas. A primeira secção refere-se ao *Switch* principal (nó central), na segunda secção aos *switches* secundários (nó intermédios), na terceira a identificação das salas e gabinetes e na última secção a descrição das salas e gabinetes.

Na primeira tabela será vista do *Switch* 1, mais respectivamente do Bloco B, Ver Tabela 18.

***Switch*1**	***Switch3***	**B101**	Sala de aula
		B102	Sala de aula
		B103	Sala de aula
		B104	Lab de Fisioterapia 1
		B105	Lab de Fisioterapia 2
		B110	Sala de aula
		B111	Sala de aula
	Switch4	**B112**	Reprografia
		B113	Lab Rádio
		B114/B115	Anfiteatro
		B116/117	Anfiteatro
		B122	Lab televisão
	Switch5	**B201**	Sala de aula
		B202	Sala de aula
		B203	Sala de aula
		B204	Lab Arquitectura
		B205	Sala de aula
		B210	Sala de aula
		B217	Sala de aula
		B218	Sala de aula
		B219	Sala de aula
		B220	Sala de aula
	Switch6	**B211**	Sala de Docentes
	Switch7	**B212**	Lab de Ensino a Distancia
	Switch8	**B213**	Lab de Informática
	Switch9	**B214**	Sala de aula
		B215	Lab de imprensa
	Switch10	**B216**	Divisão Tecnológica

Tabela 17 – Descrição dos *Switches* do Bloco B

O mesmo é descrito no Bloco A como mostra a Tabela 19.

Switch2	***Switch11***	**A101**	SAA /RH
		A102	Telefonista
		A103	Lab Física
		A105	Auditório
		A107	Lab Química
		A108	Lab Biologia
		A110	Tesouraria
	Switch12	**A113**	Bar / Refeitório
	Switch13	**A119**	CDE
	Switch14	**A201**	SFS
		A202	Unidade
		A203	GEP
		A204	Sala de Docentes
	Switch15	**A205**	Lab de Informática
	Switch16	**A206**	Lab de Informática
	Switch17	**A210**	Lab de Informática
	Switch18	**A211**	Lab de Informática
	Switch19	**A214**	Administrador
		A215	Serviço Administrativo
		A216	Reitor
		A217	Sala de Reunião
	Switch20	**A218**	Mediateca

Tabela 18 – Descrição dos Switches do Bloco A

No nível de arquitectura o mesmo será apresentado pela Figura 15.

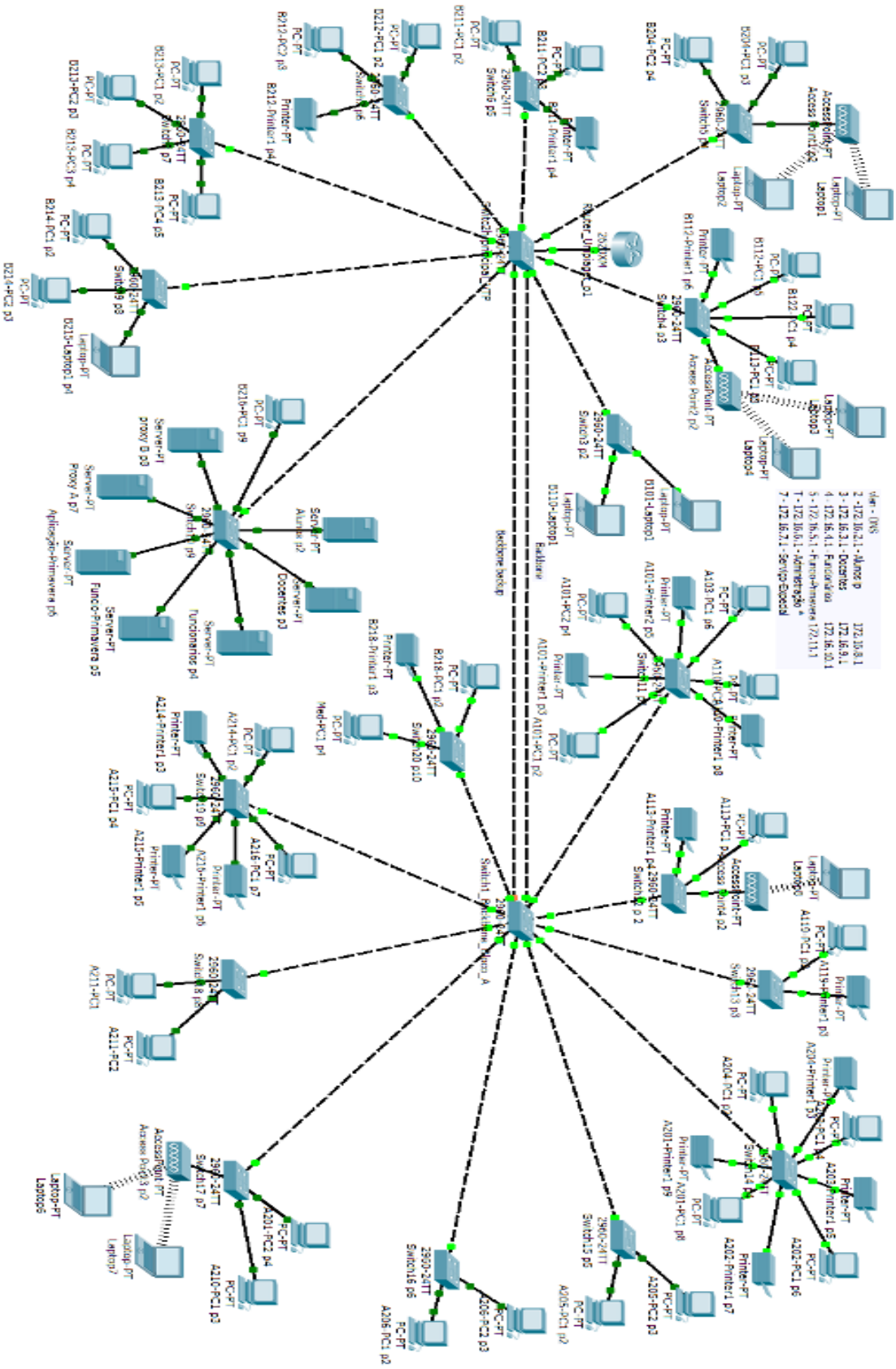


Figura 15 – Arquitectura da Rede na UniPiaget com Vlan

5.4 Configuração do *Switch Catalyst 2960 series*

Como foi referido nos capítulos anteriores, o *switch catalyst 2960 series* suporta a tecnologia de *VLAN* baseado em portas. Sendo ela inicial configura por via cabo console como mostra na Figura 16:

```
         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Switch]: Switch01

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: 123

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: 123
% Please choose a password that is different from the enable secret
  Enter enable password: 321

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: 321
```

Figura 16 – Configuração Básica do Switch

Primeiro é pedido se quer ser feito a configuração Básica. Digitamos "*yes*" e a tecla "*Enter*". Depois é solicitado os dados básicos, como o nome do dispositivo "*host name*" bem como a palavra-chave para imagem para *boot*, activar modo privilégio e para *Telnet.*

Na figura Figura 17 é demonstrado como é configurado a interface da *Vlan1* (por defeito ou *Vlan* nativo), de modo que este tenha um endereço de modo a que conseguimos conectar ao *switch* via *Telnet* e/ou via *Browser*. Deste modo o controlo e monotorização podem ser feitos a distância. Como foi referido no Capitulo 2, a Vlan native é a *Vlan* por defeito e é

responsável para a transmissão dos dados por via dos troncos (trunk) usando encapsulamento *ISL* ou *802. 1Q*. Por defeito a *interface* da *Vlan1* usa o encapsulamento *802. 1Q*.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Vlan1
Switch(config-if)#ip address 172.17.0.4 255.0.0.0
Switch(config-if)#no shutdown


%LINK-5-CHANGED: Interface Vlan1, changed state to up
Switch(config-if)#exit
Switch(config)#end

%SYS-5-CONFIG_I: Configured from console by console
Switch#
```

Figura 17 – Configuração da interface da Vlan1

Para uma melhor utilitário no uso dos encapsulamentos, é demonstrado Figura 18 os comandos para activação, mudança de encapsulamento, apresentação de informação e desativação.

Switch(config-if)#**switchport mode trunk**	Activa *trunking* na interface
Switch(config-if)#**switchport trunk encapsulation dot1q** Switch(config-if)#**switchport trunk encapsulation isl**	Define o protocolo de *trunking a usar* (Apenas em switchs com suporte a serviços no nível 3 – ex: Cisco Catalyst 3550). O 2950 apenas suporta 802.1q
Switch(config-if)#**switchport mode access**	Desactiva o *trunking* na porta actual
Switch#**show interfaces trunk** Switch#**show interfaces fa0/1 trunk**	Apresenta informação relacionada com o *trunking*

Figura 18 – Configuração de encapsulamento
Fonte: adaptado de (Sousa & Pereira, 2007/2008)

Depois disso, podemos aceder ao *switch* por três vias. Sendo elas via protocolo *Telnet, Console* e/ou via *Browser* através do protocolo *http*.

Para configuração, adição, remoção, alteração de *Vlan* usaremos o protocolo *Telnet* ou *Console*, mas para monotorização e algumas configurações básicas usaremos o protocolo *Http.*

Via *Browzer* é simplesmente inserir o *ip* do *switch* na barra de endereço e aparecerá uma janela para pedir *User Name* e *Password,* como mostra a Figura 19.

Por defeito é usado a porta 80 e *Usar Name* é admin.

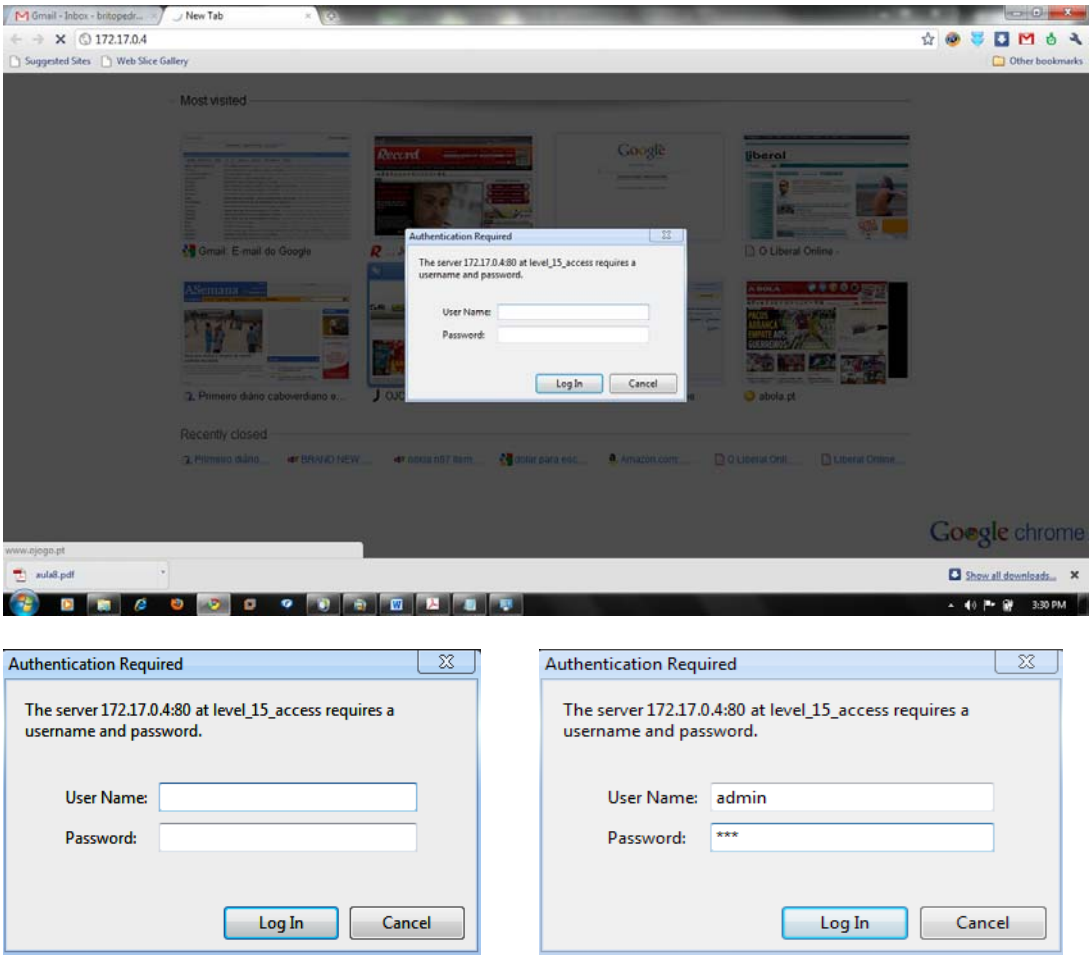


Figura 19 – Pedido de Autenticação via *Browser*

Depois do *Login* correcto temos a vista da tela Principal onde pode fazer toda a monotorização e gestão mínima necessária, como pode ser confirmado na Figura 20.

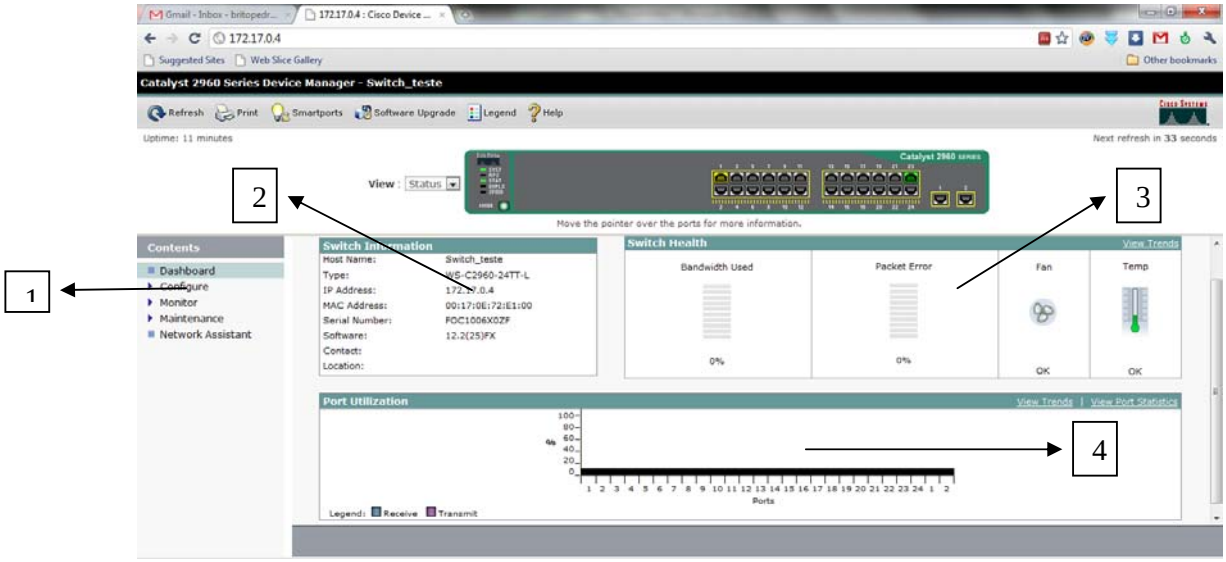


Figura 20 – Menu Principal via *Browser*

1 – Menu de Conteudos

2 – Informações do Dispositivo

3 – Informações da Rede

4 – informações de Transferencia de informação

Como foi descrevido na Figura 20, o menu principal a presenta inicialmente um conjunto de informações, desde de informações do dispositivo até infor mação da rede e de dados transimitidos.

O menu de conteudos se encontra dividida em trés sectores distintas, tendo cada uma delas uma funcionalidade propria. Para uma melhor compreensão estão apresentados na seguinte Figura 21.

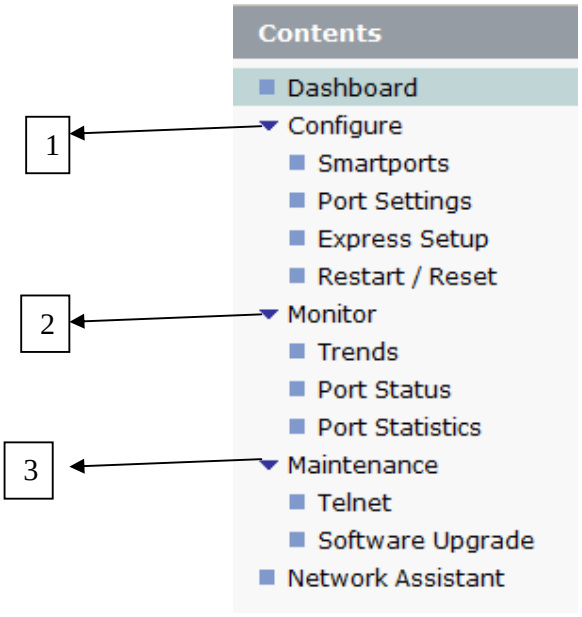


Figura 21 – Menu de Conteúdos via *Browser*

1 – Configuração

2 – Monotorização

3 – Manutenção

Dentro do Menu de conteúdos encontrasse todos os mecanismos necessários para a gestão, configuração, monotorização e manutenção do *Switch Catalist 2960 Series.* Iremos ver detalhadamente o sector configuração.

A configuração apresenta 4 sectores, como podem ser vista na Figura 21.

i. *Smartports* – onde podemos configurar de uma forma quase automática a ligação das portas com os dispositivos. Ver Figura 22.

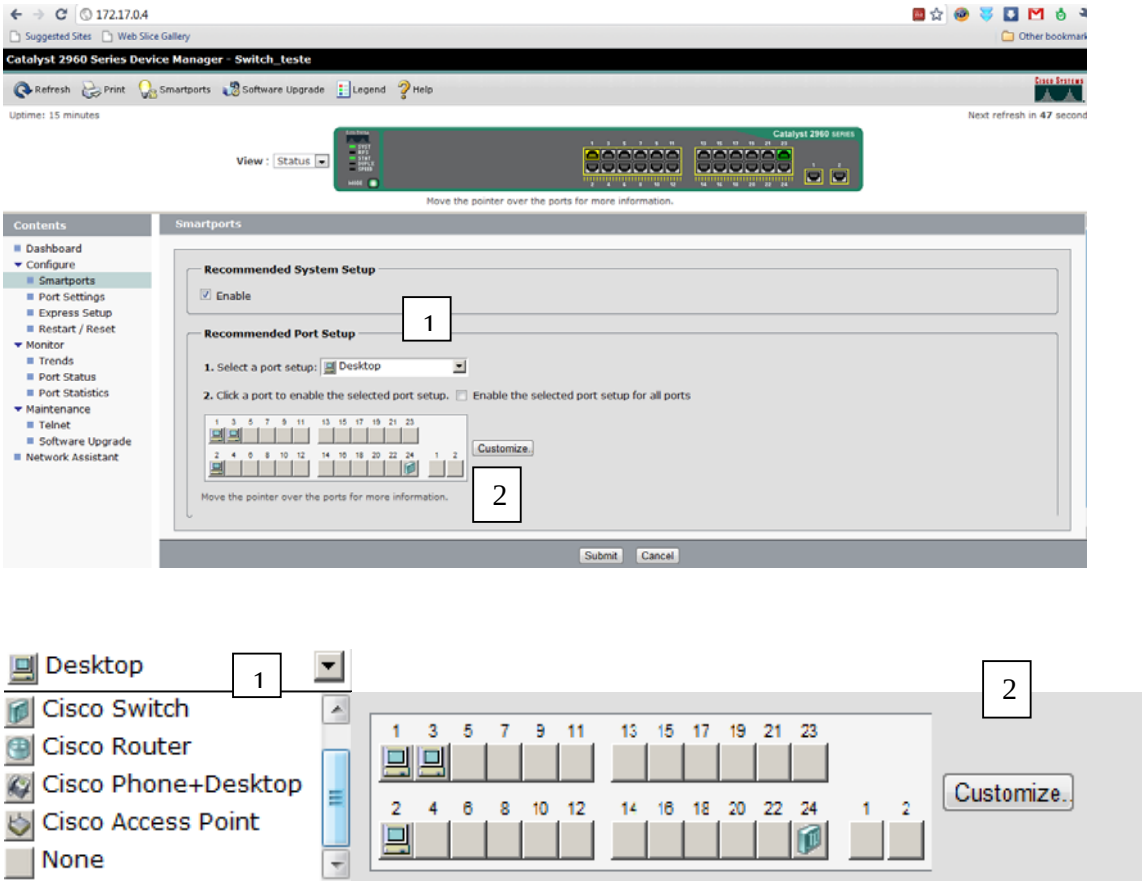
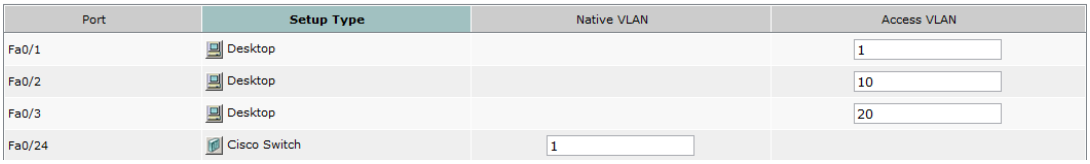


Figura 22 – Submenu de Configuração via *Browser*

E clicando no botão *Customize* podemos associar directamente cada porta a sua respetiva *VLAN*, como é demonstrado na Figura 23.



Port	Setup Type	Native VLAN	Access VLAN
Fa0/1	Desktop		1
Fa0/2	Desktop		10
Fa0/3	Desktop		20
Fa0/24	Cisco Switch	1	

Figura 23 – Configuração via *Customize*

ii. *Port Settings* – nesse sector, podemos decrever cada porta de uma forma que tudo fica orgamizado e documentado. Também tem a possiblilidade de desligar/ligar e definiar a velocidade de transmição de cada porta , ver Figura 24.

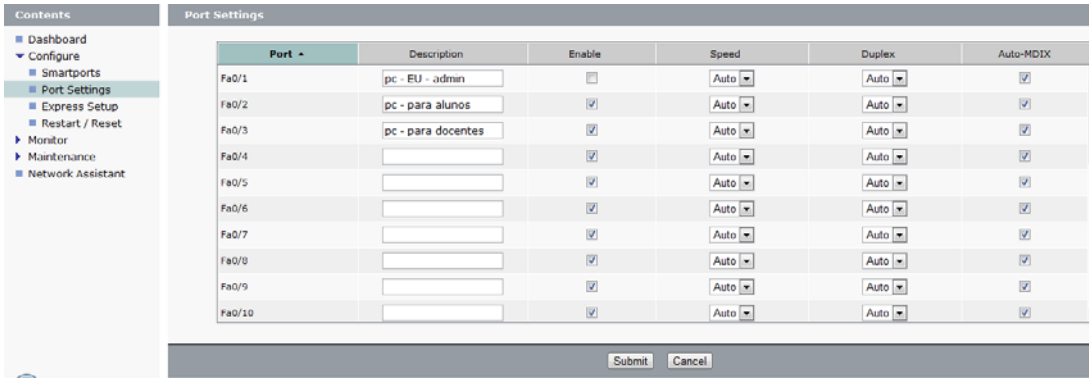


Figura 24 – Submenu *Port Settings*

iii. *Express Setup* – nesse sector, encontrasse as configurações básicas do *Switch*, deste do *host name*, até configurações de *ip address* e telnet, entre outros. Na Figura 25 podemos ver a sua interface, bem como as suas configurações.

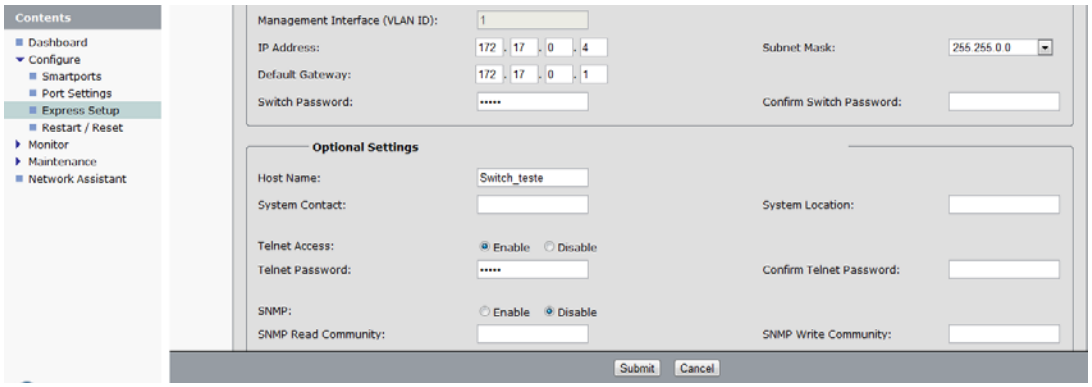


Figura 25 – Submenu *Expess Setup*

iv. *Restar/Reset* – como o próprio nome indica este sector permite reiniciar o switch. Contudo o seu reinício está dividido em duas partes. A primeira permite que os *switch* reiniciar com todas as suas configurações, a segunda faz reset de todas as configurações, ver Figura 26.

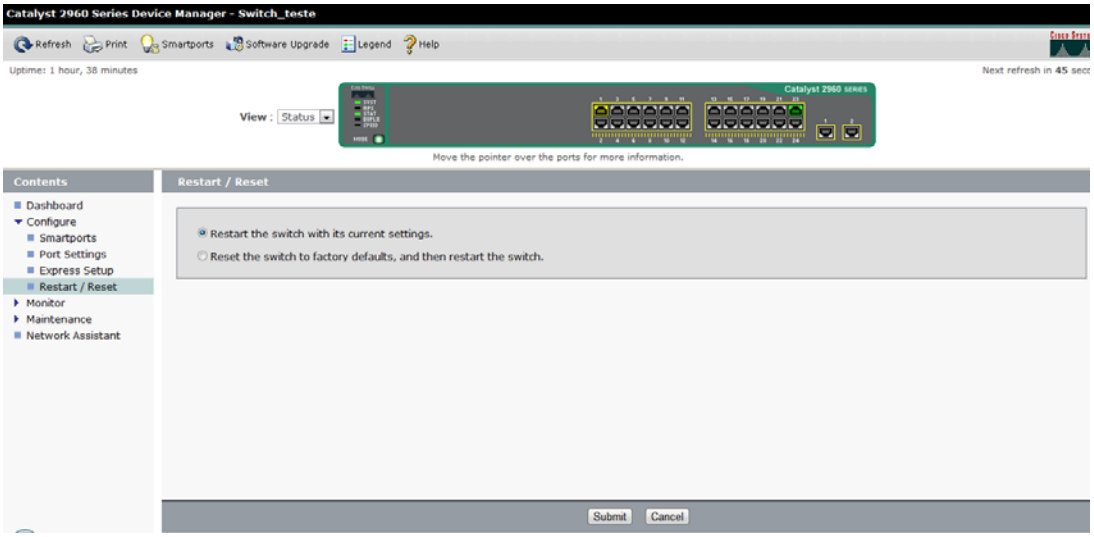


Figura 26 – Submenu *Restar/Reset*

5.5 Gestão, monotorização e manutenção de *Vlan*

A gestão, monotorização e manutenção da *Vlan*, é um dos processos mais importante em todos os processos mencionados ao longo desse projecto. O seu mau uso pode designar o insucesso de uma rede, bem como a impossibilidade de localizar a origem das falhas.

Primeiro falaremos da gestão. Para uma melhor gestão, é usado o protocolo *VTP* (Ver o Capitulo 2.6 - Protocolo de Configuração e Manutenção de *VLAN* - *VTP*), e este e usado pelo protocolo *Telnet*, ou por via *Console*. No início precisamos definir qual dos *Switches* será do modo *Server* e qual serão *Client*. Deste modo qualquer adição, Alteração, remoção de *VLAN* feito no *Switch-Server* será reencaminhado para todos os outros *Switches*.

Para uma melhor gestão, foi determinado que o *Switch1* fica no modo *Server* e os restantes ficam no modo *Client*, e todos pertencerão a um só domínio designado “UniPiaget”, como é demonstrado na Figuras 27 e Figura 28.

```
Switch>enable
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vtp server
Device mode already VTP SERVER.
Switch(vlan)#vtp domain UniPiaget
Changing VTP domain name from NULL to UniPiaget
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : UniPiaget
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB4 0x84 0x91 0x7B 0xA7 0x3B 0xB7 0xA4
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

Figura 27 – *VTP mode Server*

Como foi demostrado na Figura 27, todos os *Switches* vem por defeito no modo *Server*, mas a designação do domínio é nula. Por isso temos de designar o domínio como é mostrado na Figura nº 27. Uma vez que a ligação de *switch* para *switch* é feito no modo *Trunk*, todos *switches* mudam o seu domínio para a qual é designada pelo *Switch-Server*. Na Figura 28, podemos ver a configuração do *Switch* para o modo *Client* usando o comando "*Show Vlan Status"*. Também podemos constatar que o domínio foi alterado de "*Null*" para "*UniPiaget*" por via do *switch-Server*.

```
Switch>enable
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vtp Client
Setting device to VTP CLIENT mode.
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : UniPiaget
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB4 0x84 0x91 0x7B 0xA7 0x3B 0xB7 0xA4
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Switch#
```

Figura 28 – *TVP* modo Client

Para monotorização e manutenção ussaremos o protocolo "*http"* atravez do *browser*. Nela a monotorização pode ser feita por via interface "*Web"*, sendo ainda as informações apresentando em graficos de evolução da rede. Isto permite uma leitura mais facil e conpreensivel da situação actual da rede, bem como o transmição de pacotes que nela circulam. O menu de monotorização é subdivida em trés sectores, sendo elas as seguintes:

i. *Trends* – onde é domonstrado em gráficos a evolução da rede, bom como dos pacotes perdidos. Tambem podemos ver a transmição de pacotos de um porta, desde dos pacotes transmitidos, até os recebidos, ver Figura 29.

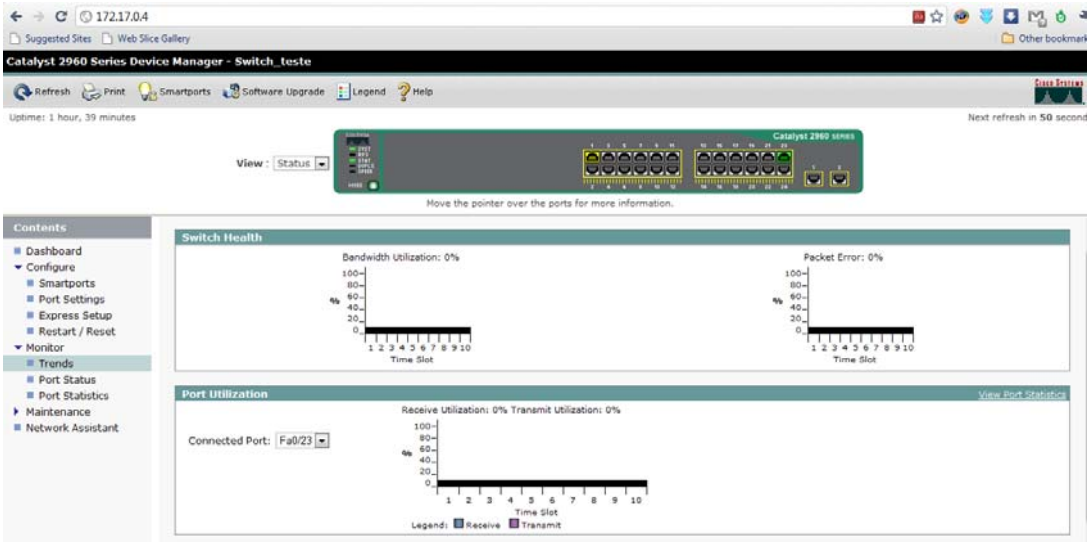


Figura 29 – Submenu *Trends*

ii. *Port Status* – permite ver a situação das portas bem como as saus descrições, vlan associadas, estados que encontram, bem como entre outros. De uma forma mais resumido, ela dá a descrição geral das portas , ver Figura 30.

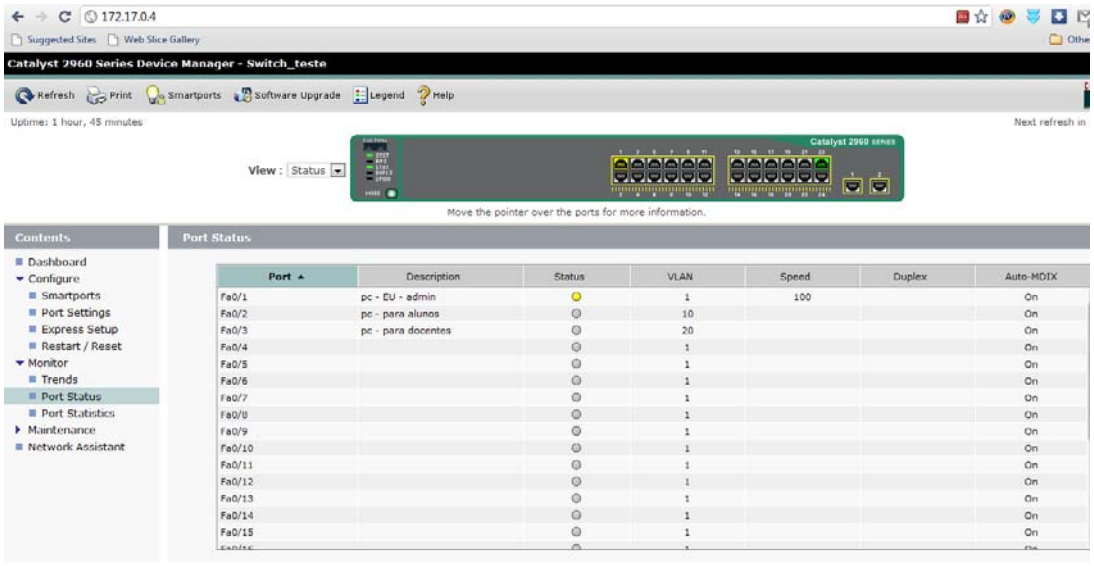


Figura 30 – Submenu *Port Status*

iii. *Port Statiscis* – nesse sector é descrito a transmissão e recepção de dados de todas as portas do *Switch.* Nela podemos ver o número de pacotes transmitidos pela uma determinada porta, número de erros de transmissão/recepção, de pacotes, como é demonstrado na Figura 31.

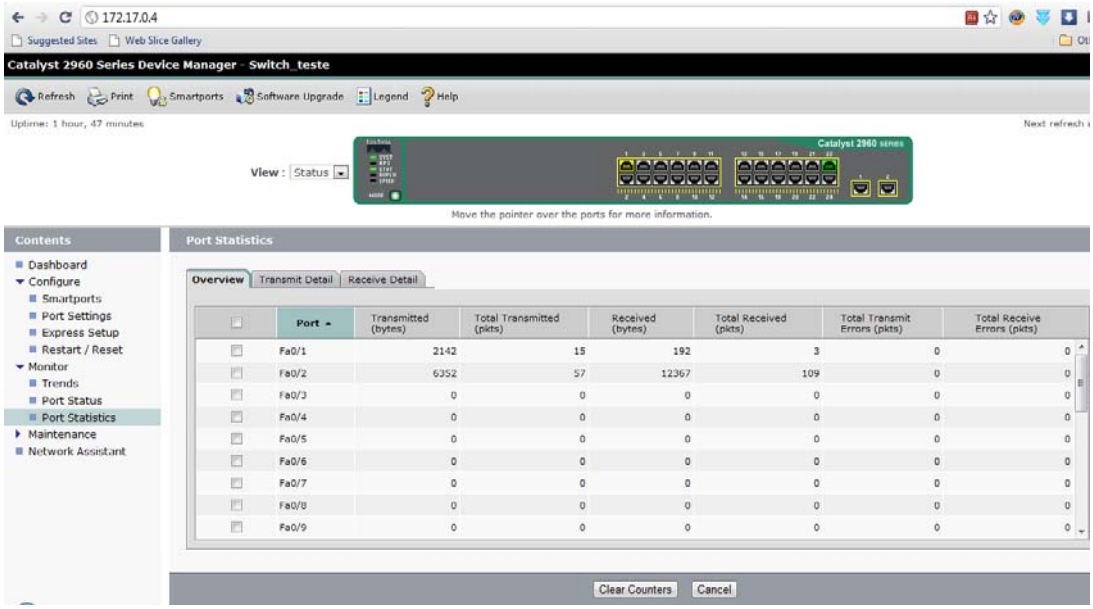


Figura 31 – Submenu *Port Statistics*

Conclusão

As *LANs* são as infra-estruturas básicas mínimas para um bom funcionamento de uma organização. Por isso a monotorização e gestão das *LANs* é um processo de extrema importância e ocupa uma boa parte do tempo do administrador da rede. Por ser uma tarefa constante e necessária, houve a necessidade de criar uma nova tecnologia, que faz isso de uma forma simples.

No âmbito desse trabalho científico, vem a necessidade de apresentar uma proposta de criação de *VLANs* para a rede universidade Jean Piaget de Cabo Verde de modo a este dar respostas a necessidade há exigências da rede actual.

Essa proposta da resposta à rede universidade, apresentando um conjunto de requisitos de forma auxiliar a gestão e monotorização da rede em causa. Nela se encontra descrição de perfil das *VLANs*, a descrição de cada uma das *VLANs* criadas, descrição da topologia, e por último a descrição dos mecanismos da gestão e de monotorização.

A implementação de *VLAN* na universidade Jean Piaget de Cabo Verde é uma necessidade básica e sua implementação é de extrema importância de modo a dar suporte necessário às exigências da rede actual. A rede universitária vem já algum tempo a sofrer algumas deficiências na sua utilização e com a implementação das *VLANs* essas deficiências serão eliminados.

As *VLANs* é a tecnologia que irá revolucionar a estrutura da rede universitária, trazendo com ele um conjunto de mecanismos de gestão e monotorização, elevando os níveis de segurança na rede. Nesses mecanismos os que mais destacas e protocolo *VTP* e o uso de interface *Web*.

O Protocolo *VTP* traz consigo um conjunto de mecanismos que permitem a gestão de *VLANs* de uma for centralizada e precisa, enquanto a interface *Web* apresenta um conjunto de mecanismos para a monotorização da rede. Todos estes mecanismos são de simples compreensão e de simples interpretação.

Para um bom funcionamento das *VLANs* na universidade Jean Piaget de Cabo Verde foi criado um perfil de cada *VLAN*, cada uma com as suas características e funcionalidades próprias. Com base nesse perfil foi elaborado as arquitecturas das *VLANs* de modo a que este se encontra com a realidade da instituição. O perfil elaborado é independente da topologia escolhida para a implementação da *VLANs*, baseasse essencialmente há necessidade de uso de elementos da rede. A divisão de segmentos permite estruturar melhor a rede, identificar melhor as falhas da rede, e aumentar a performance da rede.

Como foi demostrado no capítulo das *VLANs* no subcapítulo 4, estão descritos algumas das vantagens no uso das *VLANs*. Tendo esses atributos pode-se confirmar que as *VLANs* só trazem vantagens para a rede da organização. Ela reduz custos, reagrupa a rede, faz a monitoriza e gestão da rede, simplifica a estrutura, e aumenta a eficácia e eficiência na transferência de dados de um dispositivo para outro dispositivo. O perfil elaborado responde a necessidade da organização, mas contudo é bom salientar se o mesmo pretende investir um pouco mais, é recomendado o uso da topologia baseado em endereço *MAC*.

Em relação a proposta da *VLAN* na universidade Jean Piaget, este vai proporcionar uma maior eficácia e eficiência na rede tornando-a mais segura e mais estável. Representa um grande ganho para a instituição, e deixa à disponibilidade do administrador da rede um conjunto de mecanismos integrados para a gestão e monotorização da rede. Na proposta encontra-se como esta pode ser bem estruturada e construída, como se encontram disponíveis os dispositivos, bem como o número de *Switch* necessários para implementação do mesmo. Nela encontra-se também as principais configurações de monotorização e gestão da rede, de uma forma simples, estruturada, e centralizadas.

Em suma, a tecnologia da *VLAN* vai apresentar uma nova evolução tecnológica para a rede universitária, trazendo com ela um conjunto de vantagens e benefícios, dando estabilidade e flexibilidade na gestão e monotorização da rede. Traz ainda com uma proposta de perfil da rede universitária, dividido em domínios lógicos com cada uma delas com as suas características próprias, e por último e adaptável tanto pela topologia baseado em porta bem como baseado em endereço *MAC.* O controlo e maior fluxo de dados serão os maiores ganhos conseguidos pela organização, na implementação dessa tecnologia, sem esquecer a eliminação dos domínios de *broadcast* quase por completo.

A topologia baseada em porta apresenta características bastantes interessantes na sua implementação à rede universitária, adaptando sem muitas dificuldades a realidade que esta organização apresenta no momento, e deixando a porta aberta para as necessidades do futuro.

O perfil das *VLANs* e toda a base dessa implementação, nela encontra-se toda a informação necessária para a criação de segmentos e domínios lógicos, para uma bom funcionamento das *VLANs*, na rede universitária.

A implementação da tecnologia da *VLAN* na universidade Jean Piaget de Cabo Verde pode ser considerado uma necessidade básica necessária, e com forte impacto na resolução e identificação de problemas da rede, levando a rede universitária, a outra estado de evolução, onde controlo e gestão centralizado são a chave do sucesso. A proposta apresentada, traz consigo um perfil independe da topologia escolhida, mas que consegue responder as necessidades da universidade Jean Piaget, tanto a nível de gestão, monotorização, eficiência, eficácia, ou seja mais uma ferramenta para o administrador da rede, atingir o nível de satisfação exigida de uma rede.

Glossário

ASCII – em português - Código Padrão Americano para Intercâmbio de Informações. É um esquema de codificação de caracteres com base na ordenação do alfabeto Inglês.

Backbone – em português – rede de transporte. É a designação de esquemas de ligações centrais de um sistema mais amplo, tipicamente de elevado desempenho.

Broadcast - Broadcast ou Radiodifusão é o processo pelo qual se transmite ou difunde determinada informação, tendo como principal característica que a mesma informação está sendo enviada para muitos receptores ao mesmo tempo. Este termo é utilizado em telecomunicações e em informática.

Byte - É um dos tipos de dados integrais em computação. É usado com frequência para especificar o tamanho ou quantidade da memória ou da capacidade de armazenamento de um certo dispositivo, independentemente do tipo de dados armazenados. A codificação padronizada de byte foi definida como sendo de 8 bits. O byte de 8 bits é mais comummente chamado de octeto no contexto de redes de computadores e telecomunicações.

DNS – em português – Sistema de Nomes de Domínios. Serviço de pesquisa de nomes na Internet cuja principal utilidade é a obtenção dos endereços IP dos equipamentos que

integram a rede a partir dos nomes dos domínios. Este serviço é habitualmente designado "serviço de resolução de nomes de domínio".

EBCDIC - é uma codificação de caracteres 8 bit que descende directamente do código BCD com 6 bit e foi criado pela IBM como um padrão no início dos anos 1960 e usado no ibm 360.

Endereço IP - Endereço de 32 bits de um computador ou outro dispositivo ligado à Internet, representado habitualmente por uma notação decimal de quatro grupos de algarismos separados por pontos. Exemplo: 172.16.1.1

Endereço MAC - Endereço físico da interface de rede. É um endereço de 48 bits, representado em hexadecimal. O protocolo é responsável pelo controlo de acesso de cada estação de trabalho à rede Ethernet. Este endereço é o utilizado na camada 2 do Modelo OSI.

ETHERNET - É a tecnologia de interconexão para redes locais - Rede de Área Local (LAN) - baseada no envio de pacotes. Ela define cabeamento e sinais eléctricos para a camada física, e formato de pacotes e protocolos para a camada de controle de acesso ao meio (Media Access Control - MAC) do modelo OSI. A Ethernet foi padronizada pelo IEEE como 802.3.

FCS – em português - Sequência de verificação de um quadro. Refere-se ao extra checksum caracteres adicionado a um frame em um protocolo de comunicação para a detecção e correcção de erros . Os quadros são usados para enviar dados das camadas superiores e, finalmente, os dados do usuário da aplicação de uma fonte para um destino. O pacote de dados inclui a mensagem a ser enviada, ou dados de aplicativo do usuário. Bytes extra podem ser adicionados para quadros têm um comprimento mínimo para fins de cronometragem.

FDDI – Padrão estabelecido pelo ANSI (American National Standards Institute) em 1987. Este abrange o nível físico e de ligação de dados (as primeiras duas camadas do modelo OSI).

FTP – em português - Protocolo de Transferência de Ficheiros. Protocolo para permitir e controlar a cópia de ficheiros, normalmente via Internet. Tipicamente, quando se fala em

"programas FTP", está a fazer-se uma referência a programas que permitem copiar ficheiros de um computador para outro, via Internet.

HDLC – É um protocolo de orientada a síncrona de dados de camada de enlace. Protocolo desenvolvido pela International Organizational for Standartion (ISO).

HTTP – em português - Protocolo de Transferência de Hipertexto. Protocolo utilizado para transferência de páginas Web de hipertexto. É o protocolo de comunicação da World Wide Web (WWW).

Hub - São dispositivos concentradores, responsáveis por centralizar a distribuição dos quadros de dados em redes fisicamente ligadas em estrelas. Funcionando assim como uma peça central, que recebe os sinais transmitidos pelas estações e os retransmite para todas as demais.

IEEE 801.1Q - é uma implementação baseada em padrões da indústria de carring tráfego de múltiplas *VLAN*s em uma única interface de *trunking* entre dois *switches* Ethernet. 802.1Q é para redes Ethernet.

IEEE 802.1Q - foi desenvolvido para resolver problemas de transformação de endereços com altas taxas de dados em pequenas partes, tanto para o tráfego de Broadcast como para o de Multicast. Fazendo com que usem somente o necessário da largura de banda. Esse padrão também auxilia na segurança entre todos os segmentos da rede.

Internet - Rede alargada que é uma confederação de redes de computadores das universidades e de centros de pesquisa; do Governo, militares e comerciais, com base no protocolo TCP/IP. Proporciona acesso a sítios Web, correio electrónico, sistemas de boletins electrónicos, bases de dados, grupos de discussão, etc.

ISL - é um Cisco Systems protocolo proprietário que mantém *VLAN* informações em Ethernet quadros como os fluxos de tráfego entre os switches e roteadores ou switches e interruptores. ISL é a marcação de VLAN protocolo da Cisco e é suportado apenas em alguns

equipamentos Cisco mais rápida e links Gigabit Ethernet. Ele é oferecido como uma opção para o IEEE 802.1Q padrão.

ISO – em português – Organização Internacional para Padronização/Normalização - é uma entidade que actualmente congrega os grémios de padronização/normalização de 170 países. Funda em 23 de Fevereiro de 1947, em Genebra, na Suíça, a ISO aprova normas internacionais em todos os campos técnicos.

LAN – em português – Rede local. É uma rede de computadores que conecta computadores e dispositivos em uma área geográfica limitada, como casa, escola, laboratório de informática ou escritório.

MIME – em português - Extensões Multifunção para Mensagens de Internet. É uma norma da internet para o formato das mensagens de correio electrónico. A grande maioria das mensagens de correio electrónico são trocadas usando o protocolo SMTP e usam o formato MIME. As mensagens na Internet tem uma associação tão estreita aos padrões SMTP e MIME que algumas vezes são chamadas de mensagens SMTP/MIME.

Modelo OSI – em português – modelo de interconexão de sistemas abertos. Divide as redes de computadores em sete camadas, de forma a se obter camadas de abstracção. Cada protocolo implementa uma funcionalidade assinalada a uma determinada camada.

Modem – vem da junção das palavras modulador e demodulador. Ele é um dispositivo electrónico que modula um sinal digital em uma onda analógica, pronta a ser transmitida pela linha telefónica, e que demodula o sinal analógico e o reconverte para o formato digital original.

Multicast - é a entrega de uma mensagem ou informações a um grupo de computadores de destino simultaneamente em uma única transmissão da fonte de criação de cópias automaticamente em outros elementos de rede.

NFS – em português – Rede de sistemas de ficheiros. É um protocolo originalmente desenvolvido pela Sun Microsystems em 1984, Permitindo que um utilizador em um

cliente de computador para ter acesso a arquivos em uma rede de uma forma semelhante a como local de armazenamento é cessado.

NIC – em português – Interface da placa da rede. É um hardware que conecta um componente do computador a uma rede de computadores .

NVRAN – em português - Memória não volátil de acesso aleatório. É um tipo de memória que não perde seus dados mesmo sem a alimentação de energia.

PPP – Em português – Protocolo de Ponto-a-Ponto. Foi desenvolvido e padronizado através da RFC1661(1993) com o objectivo de transportar todo o tráfego entre 2 dispositivos de rede através de uma conexão física única. Embora seja um protocolo, o PPP encontra-se na lista de interfaces.

Protocolos - É uma convenção ou padrão que controla e possibilita uma conexão, comunicação ou transferência de dados entre dois sistemas computacionais. De maneira simples, um protocolo pode ser definido como "as regras que governam" a sintaxe, semântica e sincronização da comunicação. Os protocolos podem ser implementados pelo hardware, software ou por uma combinação dos dois.

Rede ATM – em português - Modo de Transferência Assíncrono (comutação e transmissão). É uma arquitectura de rede de alta velocidade orientada a conexão e baseada na comutação de pacotes de dados.

Router - é um equipamento usado para fazer a comutação de protocolos, a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si. Os Routers são dispositivos que operam na camada 3 do modelo OSI de referência. A principal característica desses equipamentos é seleccionar a rota mais apropriada para encaminhar os pacotes recebidos. Ou seja, escolher o melhor caminho disponível na rede para um determinado destino.

SMTP – em português - Protocolo de Transferência de Correio Simples. Norma de facto que rege a transmissão de correio electrónico através da Internet. A maioria dos sistemas de

correio electrónico na Internet usam o protocolo SMTP para enviar mensagens de um servidor para outro, podendo as mensagens ser recuperadas por um cliente usando, por exemplo, o protocolo POP3.

Software - suporte lógico é uma sequência de instruções a serem seguidas e/ou executadas, na manipulação, redireccionamento ou modificação de um dado/informação ou acontecimento.

Switch - É um dispositivo utilizado em redes de computadores para reencaminhar módulos (frames) entre os diversos nós. Possuem portas, assim como os concentradores (hubs) e a principal diferença entre um comutador e um concentrador, é que o comutador segmenta a rede internamente, sendo que a cada porta corresponde um domínio de colisão diferente, o que significa que não haverá colisões entre os pacotes de segmentos diferentes — ao contrário dos concentradores, cujas portas partilham o mesmo domínio de colisão.

Tags – Em português – etiqueta. É uma palavra-chave (relevante) ou termo associado com uma informação que o descreve e permite uma classificação da informação baseada em palavras-chave.

TCP - É um dos protocolos sob os quais assenta o núcleo da Internet. A versatilidade e robustez deste protocolo tornou-o adequado a redes globais, já que este verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros, pela rede.

Telnet - É um protocolo cliente-servidor usado para permitir a comunicação entre computadores ligados numa rede (exemplos: rede local / LAN, Internet), baseado em TCP.

TFTP - É um protocolo de transferência de ficheiros, muito simples, semelhante ao FTP. O TFTP é usualmente utilizado para transferir pequenos ficheiros entre "hosts" numa rede, tal como quando um terminal remoto ou um cliente inicia o seu funcionamento, a partir do servidor.

Topologia de rede - descreve como é o layout de uma rede de computadores através da qual há o tráfego de informações, e também como os dispositivos estão conectados a ela. Há várias formas nas quais se pode organizar a interligação entre cada um dos nós (computadores) da rede. Topologias podem ser descritas fisicamente e logicamente. A topologia física é a verdadeira aparência ou layout da rede, enquanto a lógica descreve o fluxo dos dados através da rede.

VLAN – é uma rede local que agrupa um conjunto de máquinas de maneira lógica e não física.

VTP – É um método mais fácil para a manutenção de uma configuração de VLAN consistente em toda a rede comutada. Usado para distribuir e sincronizar informações de identificação das VLANs configuradas em toda a rede comutada. As configurações estabelecidas em um único servidor VTP são propagadas através do enlace tronco para todos os switches conectados na rede. Os anúncios VTP são transmitidos para todo o domínio de gerenciamento a cada 5 minutos, ou sempre que ocorrer uma alteração nas configurações de VLANs.

Wan - uma rede de computadores que abrange uma grande área geográfica, com frequência um país ou continente.

Web - é um sistema de documentos em hipermédia que são interligados e executados na Internet. Os documentos podem estar na forma de vídeos, sons, hipertextos e figuras. Para visualizar a informação, pode-se usar um programa de computador chamado navegador para descarregar informações (chamadas "documentos" ou "páginas") de servidores Web (ou "sítios") e mostrá-los na tela do usuário. O usuário pode então seguir as hiperligações na página para outros documentos ou mesmo enviar informações de volta para o servidor para interagir com ele. O ato de seguir hiperligações é, comummente, chamado de "navegar" ou "surfar" na Web.

Wireless – em português – redes local sem fio. Rede local onde a transmissão de sinais é efectuada sem recorrer a fios ou a cabos como, por exemplo, através da utilização de ondas rádio.

Bibliografia

Angelescu, S. (2010). *CCNA Certification all-in-one for Dummies.* 111 River street Hoboken, NJ 07030-5774: Wiley Publishing, Inc., Indianapolis, Indiana.

Barros, O. S. (22 de Maio de 2007). *Segurança de redes locais com a implementação de VLANs.* Obtido em 2 de Agosto de 2010, de Memória Monográfica: http://bdigital.cv.unipiaget.org:8080/dspace/bitstream/123456789/69/1/Odair%20Barros%20.pdf

Cisco. (2 de Desembro de 2010). *Configuring Routing Between VLANs with IEEE 802.10 Encapsulation*. Obtido em 4 de Maio de 2011, de Cisco IOS Switching Services Configuration Guide: http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/xcfvl802.html

Cisco Systems Inc. (2003). *CCNA 3 and 4 Lab Companion (Cisco Networking Academy Program).* Cisco Press.

Farias, P. C. (25 de Novembro de 2006). *Redes Básico – Parte XX*. (www.juliobattisti.com) Obtido em 14 de 04 de 2011, de Julio Battisti: http://www.juliobattisti.com.br/tutoriais/paulocfarias/redesbasico020.asp

Gouveia, J., & Magalhães, A. (2005). *Redes de Computadores.* R. D. Estefânia, 138, R/C Dto., 1049-057 LISBOA: FCA - Editora de Informática, Lda.

Guilherme, W. (31 de Julho de 2009). *CCNA – 640-802 – Protocolo VTP (Virtual Trunk Protocol).* Obtido em 2 de Agosto de 2010, de NetIP-SEC.com.br: http://www.netip-sec.com.br/?p=601

Haffermann, L. (Novembro de 2009). *Segmentação de Redes com VLAN*. Obtido em 2 de Agosto de 2010, de Pós Graduação em Redes e Segurança de Sistemas: http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Haffermann%20-%20Artigo.pdf

Laboratorio de Ensino a Distancia (LED). (s.d.). *Historia e Factos*. (Universide Jean Piaget) Obtido em 2 de Agosto de 2010, de Universide Jean Piaget: http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=1

Laboratorio de Ensino a Distancia (LED). (s.d.). *Organização Científico-Pedagógica*. (Universidade Jean Piaget) Obtido em 2 de Agosto de 2010, de Universidade Jean Piaget : http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=4

Laboratorio de Ensino a Distancia (LED). (s.d.). *Orgãos de Governo*. (Universidade Jean Piaget) Obtido em 2 de Agosto de 2010, de Universidade Jean Piaget: http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=3

Laboratorio de Ensino a Distancia (LED). (s.d.). *Unidades Organizacionais*. (Universidade Jean Piaget) Obtido em 2 de Agosto de 2010, de Universidade Jean Piaget: http://www.unipiaget.edu.cv/index.php?pshow=mnu&p=1&s=5

Loureiro, P. (2003). *TCP/IP em Redes Microsoft.* Avenida Praia da Vitória 14 - 1000-247 LISBOA: FCA - Editora de Informática, Lda.

Lowe, D. (2008). *Networking ALL-IN-ONE DESK REFERENCE for DUMMIESL*. 111 River Street: Wiley Publisshing, Inc.

Madeira, F. (30 de Setembro de 2006). *Plugmasters*. (Plugmasters) Obtido em 2 de Agosto de 2010, de Plugmasters: http://www.plugmasters.com.br/sys/materias/337/1/VLAN-%E2%80%93-Virtual-Lan

Mendes, J. (2009). *Plano de Actividades 2009-10.* Cabo Verde, cidade da Praia: Universidade Jean Piaget de Cabo Verde.

PILLOU, J.-F. (18 de Agosto de 2009). *pt.kioskea.net* . (Kioskea) Obtido em 2 de Agosto de 2010, de Kioskea : http://pt.kioskea.net/contents/internet/vlan.php3

Pinto, P. (15 de Setembro de 2010). *Redes – Sabe o que é o modelo OSI?* (Peopleware) Obtido em 30 de Março de 2011, de Peopleware: http://pplware.sapo.pt/networking/redes-sabe-o-que-e-o-modelo-osi/

Sá, R. (2007). *Sistemas e Redes de Telecomunicações.* R. D. Estefânia, 183, R/C Dto., 1019-057 LISBOA: FCA - Editora de Informática, Lda.

Savi, W. (14 de Desembro de 2005). *Estratégia para analíse de Trafego de redes locais utilizando Vlan.* Obtido em 25 de Abril de 2011, de Trabalho acadêmico (graduação) - Universidade do Vale do Itajaí: http://siaibib01.univali.br/pdf/Willian%20Savi.pdf

Serpa, A. (14 de Maio de 2010). *VLAN (Virtual Local Area Network).* Obtido em 2 de Agosto de 2010, de NWC Network Concept, Lda.: http://www.nwc.pt/base-de-conhecimento/vlan-virtual-local-area-network?lang=

Soares, L. F., Lemos, G., & Colcher, S. (1995). *Redes de Computadores, Das LANs ,MANs e WANs às Redes ATM.* Rua Sete de Setembro, 111 -16º andar, 20050-002 Rio de Janeiro RJ Brasil: Editora Campos Ltda.

Sousa, O., & Pereira, N. (2007/2008). *VLAN (Virtual Local Area Network).* Obtido em 20 de 09 de 2010, de ISEP - Administração de Sistemas: http://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula8.pdf

Tanenbaum, A. S. (1996). *Redes de Computadores.* Rua sete de Setembro, 111 - 16º andar, 200050-002 Rio de Janeiro RJ Brasil: Editora Campus, Ltda.

Véstias, M. (2005). *Redes Cisco para Profissionais.* R. D. Estefânia, 183, R/C Dto., 1049-057 LISBOA: FCA - Editora de informática, Lda.

Webb, K. (2003). *CONSTRUINDO REDES CISCO USANDO COMUTAÇÃO MULTICAMADAS.* Pearson Education do Brasil.

Zacaron, M. A. (5 de Maio de 2007). *Universidade Estadual de Londrina.* Obtido em 2 de Agosto de 2010, de Utilizando Recursos de Switching STG e Vlan: http://www2.dc.uel.br/nourau/document/?down=562